TOPICS IN ALGEBRAIC GEOMETRY

TIM DOKCHITSER
TCC GRADUATE COURSE, SPRING 2015

Contents

Acknowledgments. Big thanks to Martin Dickson and Adam Morgan who were teaching assistants for this course. Thanks also to Alexander Betts and Sam Chow for their corrections (and please tell me if I forgot someone.)

Chapter 1. Varieties and algebraic groups

We review varieties defined over an algebraically closed field $k = \bar{k}$. In particular, we describe basic geometry of algebraic curves, and introduce algebraic groups and abelian varieties.

Lecture 1

1. Affine varieties

By *Affine space* $\mathbb{A}^n = \mathbb{A}^n_k$ we understand the set k^n with *Zariski topology*: $V \subset \mathbb{A}^n$ is closed if there are polynomials $f_i \in k[x_1, ..., x_n]$ such that

$$V = \{x \in k^n \mid \text{ all } f_i(x) = 0\}.$$

Every ideal of $k[x_1, ..., x_n]$ is finitely generated (it is Noetherian), so it does not matter whether we allow infinitely many f_i or not. Clearly, arbitrary intersections of closed sets are closed; the same is true for finite unions: $\{f_i = 0\} \cup \{g_j = 0\} = \{f_i g_j = 0\}$. So this is indeed a topology.

A closed nonempty set $V \subset \mathbb{A}^n$ is an *affine variety* if it is *irreducible*, that is one cannot write $V = V_1 \cup V_2$ with closed $V_i \subsetneq V$. Equivalently, in the topology on V induced from $\mathbb{A}^n$, every non-empty open subset of V is dense in V (Exc 1.1). Every closed set (=*affine algebraic set*) is a finite union of affine varieties.

Example 1.1. A *hypersurface* $V : f(x_1, ..., x_n) = 0$ in $\mathbb{A}^n$ is irreducible precisely when f is an irreducible polynomial.

Example 1.2. The only proper closed subsets of $\mathbb{A}^1$ are finite, so $\mathbb{A}^1$ and points are its affine subvarieties.

Example 1.3. The closed subsets in $\mathbb{A}^2$ are $\emptyset$, $\mathbb{A}^2$ and finite unions of points and of irreducible curves $f(x, y) = 0$.

With topology induced from $\mathbb{A}^n$, a closed set V becomes a topological space on its own right. In particular, we can talk of its subvarieties (irreducible closed subsets). The Zariski topology is very coarse; for example, every two irreducible curves in $\mathbb{A}^2$ have cofinite topology, so they are homeomorphic. So to characterise varieties properly, we put them into a category. A map of closed sets

$$\phi : \mathbb{A}^n \supset V \quad \longrightarrow \quad W \subset \mathbb{A}^m$$

is a *morphism* (also called a *regular map*) if it can be given by $x \mapsto (f_i(x))$ with $f_1, ..., f_m \in k[x_1, ..., x_n]$. Morphisms are continuous, by definition of Zariski topology. We say that ϕ is an isomorphism if it has an inverse that is also a morphism, and we write $V \cong W$ in this case.

A morphism $f : V \to \mathbb{A}^1$ is a *regular function* on V, so it is simply a function $V \to k$ that can be given by a polynomial in n variables. The regular functions on $V \subset \mathbb{A}^n$ form a ring, denoted $k[V]$, and clearly

$$k[V] \cong k[x_1, ..., x_n]/I, \qquad I = \{f \text{ s.t. } f|_V = 0\}.$$

Composing a morphism $\phi : V \to W$ with a regular function on W gives a regular function on V, so f determines a ring homomorphism $\phi^* : k[W] \to k[V]$, the *pullback* of functions. Conversely, it is clear that every k-algebra homomorphism $k[W] \to k[V]$ arises from a unique $f : V \to W$. In fact, $V \to k[V]$ defines an anti-equivalence of categories

Zariski closed sets $\longrightarrow$ finitely generated k-algebras with no nilpotents.

In particular, the ring of regular functions determines V uniquely.

Notation 1.4. Write $\operatorname{Spec} A$ for the algebraic set V with $k[V] \cong A$.

Now suppose V is a variety. Then $k[V]$ is an integral domain (Exc 1.3), and the anti-equivalence becomes

affine varieties over k $\longrightarrow$ integral finitely generated k-algebras.

The field of fractions of $k[V]$ is called *the field of rational functions* $k(V)$. Generally,

$$\phi : \mathbb{A}^n \supset V \quad \rightsquigarrow \quad W \subset \mathbb{A}^m$$

is a *rational map* if it can be given by a tuple $(f_1, ...f_m)$ of rational functions $f_i \in k(x_1, ..., x_n)$ whose denominators do not vanish identically on V. In other words, the set of points where ϕ is not defined is a proper closed subset of V, equivalently ϕ is defined on a non-empty (hence dense) open. So rational functions $f \in k(V)$ are the same as rational maps $V \rightsquigarrow \mathbb{P}^1$.

Naturally, V and W are said to be *isomorphic* (resp. *birational*) if there are morphisms (resp. rational maps) $V \rightleftarrows W$ whose composition, either way, is identity.

Example 1.5. The ring of regular functions on $\mathbb{A}^n$ is $k[\mathbb{A}^n] = k[x_1, ..., x_n]$, and $k(\mathbb{A}^n) = k(x_1, ..., x_n)$

Example 1.6. For $V : y^2 = x^3 + 1 \subset \mathbb{A}^2_{x,y}$, we have $k[V] = k[x, y]/(y^2 - x^3 - 1)$, and $k(V) = k(x)(\sqrt{x^3+1})$, a quadratic extension of $k(x)$.

The image of a variety under a morphism is not in general a variety: [1]

Example 1.7. The first projection $p : \mathbb{A}^2 \to \mathbb{A}^1$ takes $xy = 1$ to $\mathbb{A}^1 \setminus \{0\}$, which is not closed in $\mathbb{A}^1$.

Example 1.8. The map $\mathbb{A}^2 \xrightarrow{(xy,y)} \mathbb{A}^2$ has image $\mathbb{A}^2 \setminus \{x\text{-axis}\} \cup \{(0, 0)\}$.

The first example can be given a positive twist, in a sense that it actually gives $U = \mathbb{A}^1 \setminus \{0\}$ a structure of an affine variety. Generally, for a rational map $\phi : V \rightsquigarrow V'$ and $U \subset V$ open, say that ϕ is *regular on* U if it is defined at every point of U. (For $U = V$ it coincides with the notion of a regular map as before.) If ϕ has a regular inverse $\psi : V' \to V$ with $\psi(V') \subset U$, we can think of U as an affine variety isomorphic to V'. In the example above take $V' : xy = 1$ with $\phi(t) = (t, t^{-1})$ and $\psi(x, y) = t$.

[1] What is true is that the image $f(X) \subset Y$ always contains a dense open subset of the closure $\overline{f(X)}$ ([H] Exc II.3.19b).

Example 1.9. If $V \subset \mathbb{A}^n$ is a hypersurface $f(x_1, ...x_n) = 0$, then the complement $U = \mathbb{A}^n \setminus V$ has a structure of an affine variety with the ring of regular functions $k[x_1, ..., x_n, 1/f]$.

Many properties of V have a ring-theoretic interpretation. Two very important ones are:

The *dimension* $d = \dim V$ is the length of a longest chain of subvarieties

$$\emptyset \subsetneq V_0 \subsetneq \cdots \subsetneq V_d \subset V.$$

(For $k = \mathbb{C}$ this agrees with the usual dimension of a complex manifold.) With $k[V_i] = k[x_1, ..., x_n]/P_i$, this becomes the length of a longest chain of prime ideals

$$k[V] \supsetneq P_0 \supsetneq \cdots \supsetneq P_d \supset \{0\},$$

which is by definition the ring-theoretic dimension of the ring $k[V]$. For a variety V it is, equvalently, the transcendence degree of the field $k(V)$ over k.

Example 1.10. $\dim \mathbb{A}^n = \dim k[x_1, ..., x_n] = n$.

Example 1.11. A hypersurface $H \subset \mathbb{A}^n$ has dimension $n - 1$.

A regular function on V may be evaluated at a point $x \in V$, and the kernel of this evaluation map $k[V] \to k$ is a maximal ideal. (Conversely, every maximal ideal of $k[V]$ is of this form.)

Definition 1.12. The *local ring* $O_x = O_{V,x}$ is the localisation of $k[V]$ at this ideal. In other words,

$$O_x = \bigl\{ \tfrac{f}{g} \in k(V) \bigm| f, g \in k[V],\ g(x) \neq 0 \bigr\}.$$

This is indeed a local ring, of dimension $\dim V$, and its unique maximal ideal m_x consists of those rational functions that vanish at x. However, as opposed to other contexts (differentiable or analytic functions on manfiolds defined in the neighbourhood of a point), it captures more of the structure of the whole variety than of what happens at a point.[2] A good notion that does capture the local behaviour is the *completion*

$$\hat{O}_x = \varprojlim_n O_x/m_x^n.$$

It can be used to define singular and non-singular points:

Definition 1.13. Let $V \subset \mathbb{A}^n$ be a variety[3], of dimension d. A point $x \in V$ is *non-singular* if, equivalently,

(1) $\dim_k \frac{m_x}{m_x^2} = d$. ('$\geq$' always holds.)
(2) the completion $\hat{O}_x$ is isomorphic to $k[[t_1, ..., t_d]]$ over k.
(3) If $V : f_1 = ... = f_m = 0$, the matrix $(\frac{\partial f_i}{\partial x_j}(x))_{i,j}$ has rank $n - d$.

We say that V is *regular* (or *non-singular*) if every point of it is non-singular.

[2] For example, if $O_{X,x} \cong O_{Y,y}$ as rings, than X and Y are birational to one another. This is again an example of open sets being 'too large' in Zariski topology.

[3] or, say, an algebraic set all of whose irreducible components have dimension d.

Example 1.14. The curves $C_1 : y = x^2$ and $C_2 : y^2 + x^2 = 1$ in $\mathbb{A}^2$ are non-singular, and $C_3 : y^2 = x^3$ and $C_4 : y^2 = x^3 + x^2$ are singular at $(0, 0)$.

It follows from (3) that the set of non-singular points $V_{ns} \subset V$ is open (Exc 1.5), and it turns out it is always non-empty ([H] Thm. I.5.3); in particular, it is dense in V.

Finally, there are products in the category of varieties, and they correspond to tensor products of k-algebras. In other words, if $V \subset \mathbb{A}^m$ and $W \subset \mathbb{A}^n$ are closed sets (resp. varieties) then so is $V \times W \subset \mathbb{A}^m \times \mathbb{A}^n = \mathbb{A}^{m+n}$, and $k[V \times W] \cong k[V] \otimes_k k[W]$.[4]

Exc 1.1. Show that a topological space is irreducible if and only if every non-empty open subset is dense in it.
Exc 1.2. Explain why the Zariski topology on $\mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1$ is not the product topology.
Exc 1.3. Prove that for an affine variety V, the ring $k[V]$ is an integral domain.
Exc 1.4. Take the curves $C : y^2 = x^3$, $D : y^2 = x^3 + x^2$ and $E : y^2 = x^3 + x$ in $\mathbb{A}^2_k$, and the point $p = (0, 0)$ on them. Prove that $\hat{\mathcal{O}}_{C,p} \cong k[[t^2, t^3]]$, $\hat{\mathcal{O}}_{D,p} \cong k[[s, t]]/st$, $\hat{\mathcal{O}}_{E,p} \cong k[[t]]$ and that they are pairwise non-isomorphic (when $\operatorname{char} k \neq 2$).
Exc 1.5. Suppose V is given by $f_1 = ... = f_n = 0$. Using the minors of the matrix $(\frac{\partial f_i}{\partial x_j})$, prove that the set of singular points of V is closed in V.

2. Affine algebraic groups

In the same way as topological groups (Lie groups, ...) are topological spaces (manifolds, ...) that happen to have a group structure, affine algebraic groups are simply affine closed sets with a group structure.

Definition 2.1. A group G is an *affine algebraic group over k* if it has a structure of a Zariski closed set in some $\mathbb{A}^n_k$, and multiplication $G \times G \to G$ and inverse $G \to G$ are morphisms.

In other words, starting with a closed set $G \subset \mathbb{A}^n$ instead, we require

1. A point $e \in G$ (unit element),
2. A morphism $m : G \times G \to G$ (multiplication),
3. A morphism $i : G \to G$ (inverse),

which satisfy the usual group axioms[5].

Example 2.2.

1. The *additive group* $\mathbb{G}_a = \mathbb{A}^1$, group operation $(x, y) \mapsto x + y$.
2. The *multiplicative group* $\mathbb{G}_m = \mathbb{A}^1 \backslash \{0\}$, group operation $(x, y) \mapsto xy$.

[4] The hard bit is to show that $k[V \times W]$ is an integral domain, if $k[V]$ and $k[W]$ are.

[5] So $G \xrightarrow{(e,\mathrm{id})} G\times G \xrightarrow{m} G$ and (id, e) are identity maps (unit), $m \circ (m\times\mathrm{id}) = m \circ (\mathrm{id}\times m)$ as maps $G\times G\times G \to G$ (associativity), and $G \xrightarrow{\mathrm{diag}} G\times G \xrightarrow{(\mathrm{id},i)} G\times G \xrightarrow{m} G$ is the constant map $G \to \{e\}$ (inverse).

Recall that $\mathbb{A}^1 \setminus \{0\}$ is a variety via its identification with $\{xy = 1\} \subset \mathbb{A}^2$. In this notation, multiplication becomes $(x_1, y_1), (x_2, y_2) \mapsto (x_1x_2, y_1y_2)$. This example naturally generalises to GL_n (GL_1 being $\mathbb{G}_m$):

Example 2.3. Write $M_n = \mathbb{A}_{n^2}$ for the set of $n \times n$-matrices over k, and $I_n \in M_n$ for the identity matrix. The classical groups

$$\begin{array}{lcl} \mathrm{GL}_n & = & \bigl\{A \in M_n \bigm| \det A \neq 0\bigr\}, \\ \mathrm{SL}_n & = & \bigl\{A \in M_n \bigm| \det A = 1\bigr\}, \\ \mathrm{O}_n & = & \bigl\{A \in M_n \bigm| A^tA = I_n\bigr\}, \\ \mathrm{Sp}_{2n} & = & \bigl\{A \in M_{2n} \bigm| A^t\Omega A = \Omega\bigr\} \quad \bigl(\Omega = \bigl(\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\bigr)\bigr). \end{array}$$

are affine algebraic groups. This is clear for $G = \mathrm{SL}_n, \mathrm{O}_n, \mathrm{Sp}_{2n}$, because the defining conditions are polynomial in the variables, so $G \subset \mathbb{A}_{n^2}$ is closed. As for GL_n, it is the complement to the hypersurface $\det(a_{ij}) = 0$, hence affine by Example 1.9 (cf. also Exc 2.1).

A *homomorphism* of affine algebraic groups is a morphism that is also a group homomorphism, an *isomorphism* is a homomorphism that has an inverse, and *subgroups* usually refer to the ones that are closed in Zariski topology. If $H \subset G$ is any 'abstract' subgroup, its Zariski closure is a subgroup in the algebraic group sense (Exc 2.2).

It is clear that the product of two algebraic groups is an algebraic group, and that the kernel of a homomorphism $\phi : G_1 \to G_2$ is an algebraic group. It is also true that the image $\phi(G_1)$ is an algebraic group (Exc 2.3).

Example 2.4. The classical groups $G = \mathrm{SL}_n, \mathrm{O}_n, \mathrm{Sp}_n$ are subgroups of GL_n, and the embeddings $G \hookrightarrow \mathrm{GL}_n$ and the determinant map $G \to \mathbb{G}_m$ are homomorphisms.

For $g \in G$, the left translation-by-g map $l_g : G \to G$ is an isomorphism. Because these maps act transitively on G, every point of G 'looks the same'. For instance, because the set of non-singular points of G_i is non-empty, G_i is non-singular.

In particular, the irreducible components G cannot meet, and the *connected component of identity* $G^0 \subset G$ is a non-singular variety. It is a normal subgroup of G, and its left cosets are the connected components of G (Exc 2.7). So G/G^0 is finite and $G = G^0 \rtimes \Delta$ for some finite group Δ. Thus it suffices to understand connected groups; the classical matrix groups are connected (Exc 2.8).

Example 2.5. Every finite group G is an affine algebraic group, via the regular representation $G \subset \operatorname{Aut} k[G] = \mathrm{GL}_n$.

In particular, every finite affine algebraic group is a closed subgroup of some GL_n. (In fact, any faithful k-representation of G, not just the regular representation, defines such an embedding.) Somewhat surprisingly, it turns out that this is true for *all* affine algebraic groups:

Theorem 2.6. *Every affine algebraic group G is a closed subgroup of* GL_n *for some n.*

We will prove this, to illustrate that questions about affine varieties are really questions about k-algebras. First, some preliminaries are necessary.

An *action* of G on a variety V is a group action $\alpha : G \times V \to V$ which is a morphism. If $V = \mathbb{A}^n$ and the action is linear (i.e $\alpha_g : V \to V$ is in $\mathrm{GL}_n(k)$ for all $g \in G$), we say that V is a *representation* of G. Equivalently, it is a homomorphism $G \to \mathrm{GL}_n$ of algebraic groups.

To prove the theorem, we need to find $\Sigma : G \to \mathrm{GL}(V)$ whose corresponding ring map $\Sigma^* : k[\mathrm{GL}(V)] \to k[G]$ is surjective. (Then Σ is an isomorphism of G onto $\Sigma(G)$.) Putting aside the question of surjectivity, where can we possibly find a non-trivial representation in the first place?

Let us reformulate this on the level of the ring $A = k[G]$. Write[6]

$$m^* : A \longrightarrow A \otimes A, \qquad i^* : A \longrightarrow A, \qquad e^* : A \to k$$

for the ring maps corresponding to the multiplication $m : G \times G \to G$, the inverse $i : G \to G$ and the identity $e : \{\mathrm{pt}\} \to G$. To give a representation $\Sigma : G \to \mathrm{GL}(V)$ is equivalent to specifying a k-linear map

$$\sigma : V \longrightarrow V \otimes A$$

such that $(\mathrm{id} \otimes e^*) \circ \sigma = \mathrm{id}$ and $(\mathrm{id} \otimes m^*) \circ \sigma = (\sigma \otimes \mathrm{id}) \circ \sigma$. We say that σ makes V into an *A-comodule.*

There is only one obvious A-comodule, and that is $V = A = k[G]$ itself with $\sigma = m^*$, the co-multiplication map. The only problem is that $k[G]$ is an infinite-dimensional k-vector space[7], so what we need is the following

Lemma 2.7. *Every finite-dimensional k-subspace $W \subset A$ is contained in a finite-dimensional subcomodule $V \subset A$ (that is, $m^*(V) \subset V \otimes A$).*

Proof. A sum of subcomodules is again one, so we may assume $W = \langle w \rangle$ is one-dimensional. Write $m^*(w) = \sum_{i=1}^n v_i \otimes a_i$ with $a_1, ..., a_n$ linearly independent over k and complete them to a k-basis $\{a_i\}_{i \in I}$ of A. We claim that $V = \langle w, v_1, ..., v_n \rangle$ is a comodule.

Indeed, suppose $m^*(a_i) = \sum c_{ijk}\, a_j \otimes a_k$. Then

$$\sum m^*(v_i) \otimes a_i = (m^* \otimes \mathrm{id}) m^*(w) = (\mathrm{id} \otimes m^*) m^*(w) = \sum v_i \otimes c_{ijk} a_j \otimes a_k$$

in $V \otimes A \otimes A$. Comparing the coefficients of a_k, we get $m^*(v_k) = \sum v_i \otimes c_{ijk} a_j$, so $m^*(V) \subset V \otimes A$. □

Proof of Theorem 2.6. Pick some k-algebra generators of $A = k[G]$, and let $W \subset A$ be their k-span. Take an A-comodule $W \subset V \subset A$ as in the lemma,

[6] A k-algebra A with such maps m^*, i^* and e^* that satisfy the axioms $(e^* \otimes \mathrm{id}) \circ m^* = \mathrm{id}$, $(\mathrm{id} \otimes m^*) \circ m^* = (m^* \otimes \mathrm{id}) \circ m^*$ and $(i^* \otimes \mathrm{id}) \circ m^* = e^*$ (dual to the previous footnote) is called a *Hopf algebra*, and the maps *comultiplication*, *counit* and *coinverse* respectively.

[7] unless G is finite, in which case the construction recovers Example 2.5

and let $v_1, ..., v_n$ be a k-basis of V. The image of

$$\Sigma^* : k[\mathrm{GL}(V)] = k[x_{11}, ..., x_{nn}, 1/\det] \longrightarrow A$$

contains $\sum_i e^*(v_i)\Sigma^*(x_{ij}) = (e^* \otimes \mathrm{id})m^*(v_j) = v_j$, so Σ^* is surjective. □

Note that the proof is completely explicit.

Example 2.8. Take $G = \mathbb{G}_a$. Then $A = k[G] = k[t]$ is generated by t, so take $W = \langle t \rangle$. The comultiplication

$$m^* : k[t] \longrightarrow k[t] \otimes k[t] \qquad (\cong k[t_1, t_2])$$

maps $t \mapsto t \otimes 1 + 1 \otimes t$ $(=t_1+t_2)$, so $m^*(W) \not\subset W \otimes A$. In other words, W is not a comodule. But $V = \langle 1, t \rangle$ is one (cf. proof of Lemma 2.7), and the corresponding embedding $\mathbb{G}_a \to \mathrm{GL}_2$ is

$$t \longmapsto \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right).$$

In view of Theorem 2.6, affine algebraic groups are also called *linear algebraic groups*. The statement of the theorem can even be refined so that a given $H < G$ can be picked out as a stabiliser of some linear subspace:

Theorem 2.9 (Chevalley)**.** *Let $H < G$ be a (closed) subgroup of an affine algebraic group G. There is a linear representation $G \to \mathrm{GL}(V)$ and a linear subspace $W \subset V$ whose stabiliser is H.*

Proof. Exc 2.10. □

Extending this further, one proves that if $H < G$ is normal, it is possible to find V such that H is precisely the kernel of $\phi : G \to \mathrm{Aut}\, V$ (see [Wat] §16.3). The image $\phi(G)$ is then an algebraic group, so *factor groups exist* for algebraic groups. (In positive characteristic this factor group is not unique, because there are injective homomorphisms of algebraic groups that are not isomorphisms, see Exc 2.12; the question whether the quotient G/H exists in the sense of category theory is subtle, see [Wat] §15–16.)

Exc 2.1. Write down explicitly the multiplication map and the inverse for $\mathrm{GL}_2 \subset \mathbb{A}^5$.

Exc 2.2. Suppose G is an algebraic group and $H \subset G$ is a subgroup in the 'abstact group sense'. Then its (Zariski) closure $\bar{H} \subset G$ is a subgroup in the algebraic group sense.

Exc 2.3. Show that the image of an algebraic group homomorphism is an algebraic group. (The image of a variety under a morphism is not always a variety, see Exc 3.6.)

Exc 2.4. (Closed orbit lemma) Suppose $G \times V \to V$ is an action of G on a variety V, and let $U = Gv$ be an orbit. Then the closure $\bar{U} \subset V$ is a variety, $U \subset \bar{U}$ is open and non-singular, and $\bar{U} \setminus U$ is a union of orbits (of strictly smaller dimension). In particular, the orbits of minimal dimension are closed.

Exc 2.5. Let G be an algebraic group and write $\mathrm{Aut}\, G$ for the set of isomorphisms $G \to G$ (as algebraic groups). Determine $\mathrm{Aut}\, G$ for $G = \mathbb{G}_a$ and $G = \mathbb{G}_m$. Does $\mathrm{Aut}\, G$ have a structure of an algebraic group in these cases, and is it true that its action on G is an algebraic group action?

Exc 2.6. If G is a connected algebraic group and $H \lhd G$ is finite, show that H is contained in the centre of G. In particular, H is abelian.

Exc 2.7. Prove that the connected component of identity $G^0 \subset G$ is a normal subgroup and its left cosets are the connected components of G.

Exc 2.8. Show that the classical groups $\mathrm{GL}_n, \mathrm{SL}_n, \mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n$, Sp_{2n} are connected.

Exc 2.9. Do Example 2.8 for $G = \mathbb{G}_m$.

Exc 2.10. Prove Theorem 2.9 (Modify the proof of Theorem 2.6.)

Exc 2.11. A *character* of G is a 1-dimensional representation of G, equivalently a homomorphism $G \to \mathbb{G}_m$. Prove that characters are in 1-1 correspondence with invertible elements $x \in k[G]^\times$ such that $m^*(x) = x \otimes x$. What does the product of characters correspond to? Compute the character group for $G = \mathbb{G}_m$ and $G = \mathbb{G}_a$.

Exc 2.12. Let $G \subset \mathbb{A}^n$ be an affine algebraic group of dimension > 0 over $k = \bar{\mathbb{F}}_p$. Suppose G is given by the equations $f_i(x_1, ..., x_n) = 0$. For a polynomial f write $f^{(p)}$ for the polynomial whose coefficients are those of f raised to the pth power. Prove that $G^{(p)} = \{x | f_i^{(p)}(x) = 0\}$ is also an algebraic group, and that the *Frobenius map* $F(x) = x^p$ is a homomorphism from G to $G^{(p)}$. Prove that F is bijective but not an isomorphism of algebraic groups.

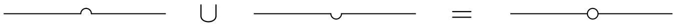
3. General varieties and completeness

Lecture 2

To define a topological (C^∞, analytic, ...) manifold one takes a topological space covered by open sets $V = \bigcup_i V_i$, such that

1. Each V_i is identified with a standard open ball in $\mathbb{R}^n$ (or $\mathbb{C}^n$).
2. The transition functions between charts $V_i \supset V_i \cap V_j \to V_j \cap V_i \subset V_j$ are continuous (C^∞, analytic,...).
3. V is Hausdorff and second countable.

The Hausdorff condition is necessary to avoid unpleasanties like glueing $\mathbb{R}$ with $\mathbb{R}$ along $\mathbb{R} - \{0\}$:



The two origins cannot be separated by open sets, so the resulting space is not Hausdorff although both charts are. We do not want this.

We now copy this definition to glue affine varieties together, and we only allow finitely many charts (replacing 'second countable').

Definition 3.1. An *algebraic set* V is a topological space covered by finitely many open sets $V = V_1 \cup ... \cup V_n$ (affine charts), such that

1. Each V_i has a structure of an affine variety.
2. The transition maps $V_i \supset V_i \cap V_j \to V_j \cap V_i \subset V_j$ are isomorphisms[8].
3. V is closed in $V \times V$ (V is *separated*).[9]

[8] That is, rational functions $\phi_{ij} : V_i \to V_j$, defined everywhere on $V_i \cap V_j \subset V_i$ and mapping it to $V_j \cap V_i \subset V_j$.

[9] The topology on $V \times V$ comes from Zariski topology on affine varieties $V_i \times V_j$ that cover it.

An *(algebraic) variety* is an irreducible algebraic set; in particular, varieties are connected.

The separatedness condition (3) is equivalent to Hausdorffness for topological spaces, but makes sense for varieties. (Because open sets are usually dense in Zariski topology, varieties are never Hausdorff.) See Excs 3.2–3.5.

We refer to 1-dimensional varieties as *curves* and 2-dimensional varieties as *surfaces*. A 0-dimensional variety is a point.

Example 3.2. If X is an affine variety and $V \subset X$ an open set, then V is general not an affine variety (unless V is a complement to a hypersurface $f = 0$ — the case we discussed before). However, X can always be covered by finitely many affine subvarieties of X, so it is a variety. Generally, both open and irreducible closed subsets of a variety are varieties (Exc 3.8).

Example 3.3. *Projective space* $\mathbb{P}^n = \mathbb{P}^n_k$ is a set of tuples $[x_0 : \cdots : x_n]$ with $x_i \in k$ and not all 0, modulo the relation that $[ax_0 : \cdots : ax_n]$ defines the same point for all $a \in k^\times$.

A subset $V \subset \mathbb{P}^n$ is closed if there are *homogeneous* polynomials f_i in $x_0, ..., x_n$ such that

$$V = \{x \in \mathbb{P}^n \mid \text{ all } f_i(x) = 0\}.$$

As f_i are homogeneous, the condition $f_i(x) = 0$ is independent of the choice of a tuple representing x.

To give $\mathbb{P}^n$ a structure of a variety, cover it $\mathbb{P}^n = \mathbb{A}^n_{(0)} \cup \cdots \cup \mathbb{A}^n_{(n)}$ with

$$\mathbb{A}^n_{(j)} \;=\; \{[x_0 : \ldots x_{j-1} : 1 : x_{j+1} : \ldots x_n]\} \;\subset\; \mathbb{P}^n$$

The transition maps between charts are indeed morphisms

$$\mathbb{A}^n_{(j)} - \{x_k = 0\} \;\longrightarrow\; \mathbb{A}^n_{(k)} - \{x_j = 0\}, \qquad (x_i) \mapsto (x_i \tfrac{x_j}{x_k}),$$

so $\mathbb{P}^n$ becomes an algebraic variety. Closed irreducible subsets of $\mathbb{P}^n$ are called *projective varieties*; see Exc 3.9.

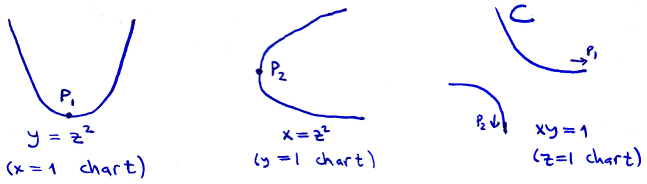
Example 3.4. The closure in $\mathbb{P}^2$ of an affine curve

$$C : xy = 1 \quad \subset \mathbb{A}^2$$

is a projective curve

$$\bar{C} : xy = z^2 \quad \subset \mathbb{P}^2.$$

Its pieces on the three standard affine charts of $\mathbb{P}^2$ are



So $\bar{C} \setminus C = \bar{C} \cap \mathbb{P}^1_{z=0}$ consists of two points $P_1 = [1 : 0 : 0]$ and $P_2 = [0 : 1 : 0]$.

A *morphism* $X \to Y$ of algebraic sets is a continuous map which is a morphism when restricted to affine charts. A *rational map* $X \rightsquigarrow Y$ is a morphism from a dense open set. As before, *regular* and *rational functions* on X as morphisms $X \to \mathbb{A}^1$ and rational maps $X \rightsquigarrow \mathbb{A}^1$, respectively. The former form a ring $k[X]$, and the latter a field $k(X)$ if X is a variety. However, unless X is affine, $k(X)$ is usually much larger than the field of fractions of $k[X]$ (Exc 3.10).

The nicest manifolds are the compact ones, but Zariski compactness is not the right notion for varieties — from finite-dimensionality it follows easily that every affine variety is compact (Exc 3.2).

Definition 3.5. A variety X is *complete* if it satisfies the following:

Lemma 3.6. *The following conditions are equivalent:*

(1) *('Universally closed') For every variety Y, the projection $X \times Y \xrightarrow{p_2} Y$ maps closed sets to closed sets*[10]*.*
(2) *('Maximality') If $X \subset Y$ is open with Y a variety, then $X = Y$.*
(3) *('Valuative criterion') For every curve C and a non-singular point $P \in C$, any morphism $C \setminus \{P\} \to X$ extends to a morphism*[11] *$C \to X$.*

In the same way as separatedness is a reformulation of being Hausdorff, the first condition defines compactness for usual topological spaces (Exc 3.11). There other two are perhaps a bit more natural — both say that X is as large as possible in some sense, and has no missing points.

Example 3.7. $\mathbb{A}^1$ is not complete:

(1) fails because under $\mathbb{A}^1 \times \mathbb{A}^1 \xrightarrow{p_2} \mathbb{A}^1$, the set $xy = 1$ projects to $\mathbb{A}^1 \setminus \{0\}$.
(2) fails because $\mathbb{A}^1$ may be embedded in $\mathbb{P}^1$ as a dense open subset.
(3) fails because $\mathbb{A}^1 \setminus \{0\} \xrightarrow{x \mapsto x^{-1}} \mathbb{A}^1$ does not extend to $\mathbb{A}^1 \to \mathbb{A}^1$.

The most non-trivial step in the equivalence is the following theorem. Recall that any topological space can be compactified, and this is the analogue:

Theorem 3.8 (Nagata)**.** *Every variety can be embedded in a complete variety as a dense open subset.*

The theorem is easy for affine varieties (embed $V \subset \mathbb{A}^n \subset \mathbb{P}^n$ and take the closure $\bar{V}$ of V in $\mathbb{P}^n$; then $V \subset \bar{V}$ is dense open and $\bar{V}$ is a projective variety, hence complete, as we will see soon). For arbitrary varieties it therefore becomes a question of arranging the completions of affine charts so that they can be glued together. This may be done using 'blowing-ups' and 'blowing-downs', so there is some non-trivial geometry involved.

Here are some immediate consequences of completeness:

Lemma 3.9. *Suppose X is a complete variety.*

(a) *If $Z \subset X$ is closed, then Z is complete.*

[10] We say that $\pi : X \to \{\text{pt}\}$ is 'universally closed' ($\pi \times \text{id}_Y$ is a closed map for all Y).

[11] necessarily unique as X is a variety and is therefore separated

(b) *For any morphism $f : X \to Y$ the image $f(X)$ is complete and closed in Y.*
(c) *$k[X] = k$, in other words X has no non-constant regular functions.*
(d) *If X is affine, then X is a point.*

Proof. (a) Clear from condition (1).
(b) $f(X)$ is the same as p_2 of the "graph of f" $(x, f(x)) \subset X \times Y$.
(c) The image of X under the composition $X \xrightarrow{f} \mathbb{A}^1 \hookrightarrow \mathbb{P}^1$ is connected, closed and misses ∞, so it must be a point.
(d) Affine varieties are characterised by $k[X]$. □

The main example of a complete variety is $\mathbb{P}^n$ (Exc 3.14). By (a), all projective varieties are therefore complete, and these are the only complete varieties we will ever encounter.[12] In fact, every complete variety X is birational to a projective variety X' via a regular (and not just rational) map $X' \to X$ (Chow's Lemma).

Example 3.10. As an application, here is a weak version of Bezout's theorem — every two curves intersect in $\mathbb{P}^2$. Indeed, if $C : f(x, y, z) = 0$ and $D : g(x, y, z) = 0$ have empty intersection, then

$$[f(x, y, z) : x^{\deg f}] : \qquad D \to \mathbb{P}^1$$

is a regular map that misses $[0 : 1]$, which is impossible unless this is a constant map, and it is clearly not.

Finally, for complete varieties there is a very close connection between the usual complex topology and Zariski topology:

Theorem 3.11 (Chow)**.** *Let X, Y be complete varieties over $\mathbb{C}$.*
(1) *Every analytic[13] subvariety of X is closed in Zariski topology.*
(2) *Every holomorphic map $f : X \to Y$ is induced by a morphism of varieties.*

Chow proved (1) for $X = \mathbb{P}^n$ and the rest of the assertions follow relatively easily (using Chow's lemma for (1) and applying (1) to the graph of f in (2); see Mumford 'Abelian Varieties' §1.3).

In particuar, the only meromorphic functions on a complete variety over $\mathbb{C}$ are rational functions (take $Y = \mathbb{P}^1$).

Exc 3.1. Prove that every curve has cofinite topology.

Exc 3.2. Every variety X is compact, and X is not Hausdorff unless X is a point.

Exc 3.3. A topological space X is Hausdorff if and only if the diagonal $X \subset X \times X$ is closed in the product topology.

Exc 3.4. ('Valuative criterion of separatedness') Suppose V satisfies (1) and (2) in the definition of an algebraic set. Then it satisfies (3) if and only if for every curve C and a

[12] In fact, complete curves and surfaces are always projective, and it is quite non-trivial to construct a non-projective complete 3-dimensional variety ('Hironaka's example', 1960).

[13] Locally (in the usual complex topology) a zero set of holomorphic functions

non-singular point $P \in C$, any morphism $C \setminus \{P\} \to X$ has at most one extension to a morphism $C \to X$.

Exc 3.5. If $f, g : X \to V$ are morphisms of varieties, the set of points $x \in X$ where $f(x) = g(x)$ is closed in X. In fact, for a fixed V this holds for all X, f, g if and only if V is separated.

Exc 3.6. Show that the image of $\mathbb{A}^2$ under $(xy, x) : \mathbb{A}^2 \to \mathbb{A}^2$ is not a variety.

Exc 3.7. Let $U \subset V$ be a non-empty open subset of an affine variety. Prove that U can be covered by affine varieties of the form $V \setminus \{f = 0\}$ (cf. Example 1.9), and can be thus given a structure of an affine variety.

Exc 3.8.

(a) Prove that $\mathbb{A}^2 - \{(0,0)\}$ is not isomorphic to an affine variety.
(b) Suppose X is an affine variety and $\emptyset \neq V \subset X$ open. Then V can be covered by finitely many affine subvarieties of X, so it is a variety.
(c) Prove that irreducible closed subsets of a variety are varieties.

Exc 3.9. Prove that $\mathbb{A}^n$ and $\mathbb{P}^n$ are varieties, that is satisfy the separatedness condition. In particular, affine varieties and projective varieties are actually varieties.

Exc 3.10. Show that $k[\mathbb{P}^1] = k$ and $k(\mathbb{P}^1) \cong k(t)$.

*Exc 3.11. A topological space X is compact if and only if $X \times Y \xrightarrow{p_2} Y$ takes closed sets to closed sets for every topological space Y.

Exc 3.12. Prove Lemma 3.6.

Exc 3.13. Let C be a curve and $P \in C$ a non-singular point. Show that the local ring $O_{C,P} \subset k(C)$ of functions defined at P is a discrete valuation ring.

Exc 3.14. Use Exc 3.13 and the 'valuative criterion' to show that $\mathbb{P}^n$ is complete.

Exc 3.15. Determine $k[\mathbb{P}^n]$ and $k(\mathbb{P}^n)$.

Exc 3.16. Show that for complex varieties that are not complete Chow's theorem may fail.

Exc 3.17. Prove that a compact complex manifold has at most one algebraic structure.

4. Curves

The power of completeness is especially visible for non-singular curves:

Lemma 4.1. *Suppose C_1 and C_2 are complete non-singular curves.*

(i) *Any morphism $C_1 \setminus \{P_1, ..., P_n\} \to C_2$ extends uniquely to $C_1 \to C_2$.*
(ii) *Every rational map $C_1 \to C_2$ extends to a (unique) morphism, and every birational map to an isomorphism.*
(iii) *Every non-constant map $f : C_1 \to C_2$ is surjective.*

Proof. (i) Existence is 3.6 (3), and uniqueness follows from separatedness of C_2. (ii) is immediate from (i). (iii) $\operatorname{Im} f$ is irreducible and closed, so it is either a point or the whole of C. □

So for non-singular complete curves there is no distinction between rational maps and morphisms, and it is not hard to deduce that $C \mapsto k(C)$ defines an (anti-)equivalence of categories

$$\begin{array}{c} \text{complete non-singular} \\ \text{curves over } k \end{array} \longrightarrow \begin{array}{c} \text{Finitely generated field extensions} \\ K/k \text{ of transcendence degree 1.} \end{array}$$

In higher dimensions this is not true — for instance $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$ have the same field of rational functions, but are not isomorphic (Exc 4.3).

For the rest of this section, curves are *non-singular complete curves.*[14] When $k = \mathbb{C}$, our curves are the same as compact Riemann surfaces. (In particular, every Riemann surface is algebraizable, that is arises from a unique such curve.)

A non-constant map of curves $\phi : C \to D$ gives an embedding of fields $\phi^* : k(D) \hookrightarrow k(C)$ of finite index (as both have transcendence degree 1), which is the *degree of* ϕ,

$$\deg \phi = [k(C) : \phi^* k(D)].$$

In particular, ϕ is an isomorphism if and only if it has degree 1.

Example 4.2. Here is an example of a morphism of degree 2,

$$\begin{array}{cccc} f: & C: x^2+y^2=1 & \longrightarrow & D = \mathbb{P}^1_x. \\ & (x,y) & \mapsto & x \end{array}$$

It corresponds to the field inclusion $f^* : k(x) \hookrightarrow k(x, \sqrt{(}1-x^2))$.
[Note: When we say '$C : x^2+y^2 = 1$' we are writing down an affine equation, but there is a unique non-singular complete curve $\bar{C}$ in which $C \subset \bar{C}$ is dense open, and this is the curve we mean. Here $\bar{C} : x^2 + y^2 = z^2 \subset \mathbb{P}^2$.]

Another way to see the degree of $f : C \to D$ is to relate it, as in topology (for covers of topological spaces) to the number of pre-images of a point of D. Using basic facts about extensions of valuations in finite field extensions, it is not hard to see that every has d pre-images counted with multiplicities, where $d = \deg \phi$ in characteristic 0, and the separable degree of $k(C)/\phi^* k(D)$ in general. All but finitely many points have exactly d distinct pre-images.

Every non-constant rational function $f \in k(C)$ is a surjective morphism $f : C \to \mathbb{P}^1$, and we say that f has a *zero* at P if $f(P) = 0$ and a *pole* at P if $f(P) = \infty$. The above discussion says that f has d zeroes and d poles, if counted with multiplicities (which is done using divisors, defined below).

The local ring $O = O_{C,P}$ of a curve C at a point $P \in C$ is a local domain of dimension 1. As P is non-singular, $\dim_k m/m^2 = 1$, forcing O to be a *discrete valuation ring.* In other words, there is a well-behaved 'order of vanishing of functions at P',

$$\mathrm{ord}_P : k(C)^\times \twoheadrightarrow \mathbb{Z},$$

which is a discrete valuation.[15] In fact, discrete valuations on $k(C)$, trivial on k, are in 1-1 correspondence with the points of C, via ord.

If $\mathrm{ord}_P(f) = 1$, we call f a *uniformizer* at P. If we pick such a uniformizer, say t, every rational function $f \in k(C)^\times$ has a unique expression

$$f = ut^n, \qquad u(P) \neq 0, \infty, \qquad n = \mathrm{ord}_P(f).$$

[14] Equivalently, they are non-singular projective curves, as for curves it is not hard to show that complete implies projective. This is also true in dimension 2 but not 3 or higher.

[15] $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$ and $\mathrm{ord}_P(f+g) \geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g))$.

Definition 4.3. A *divisor* on a (non-singular complete) curve C/k is a finite formal linear combination of points,

$$D=\sum_{i=1}^{r} n_i(P_i), \qquad n_i\in\mathbb{Z},\ \ P_i\in C.$$

The *degree* of D is $\sum n_i$, and D is *effective* (written $D\geq 0$) if all $n_i\geq 0$. We write $\operatorname{Div}^n(C)$ for the set of divisors of degree n, and $\operatorname{Div}(C)$ for all divisors.

If $f\in k(C)^\times$ is a non-zero rational function, the *divisor of* f is defined as

$$(f)=\sum_{P\in C}\operatorname{ord}_P(f)\,(P).$$

Divisors of this form are called *principal*.

It is not hard to see that principal divisors have degree 0, and they form a subgroup of the abelian group of all divisors. In fact, if $(f)=D^0-D^\infty$ with $D^0, D^\infty\geq 0$, then $\deg D^0=\deg D^\infty$ is the degree of the map $f:C\to\mathbb{P}^1$.

Definition 4.4. The quotient groups

$$\operatorname{Pic} C=\frac{\text{divisors on C}}{\text{principal divisors}}, \qquad \operatorname{Pic}^0 C=\frac{\text{divisors of degree 0 on } C}{\text{principal divisors}}$$

are called the *Picard group of* C and the *degree 0 Picard group of* C. Two divisors are called *linearly equivalent* if they have the same class in $\operatorname{Pic} C$.

There is an obvious (split) exact sequence

$$0\longrightarrow \operatorname{Pic}^0 C\longrightarrow \operatorname{Pic} C\overset{\deg}{\longrightarrow}\mathbb{Z}\longrightarrow 0.$$

Lecture 3

Exc 4.1. Suppose C is a curve.

(a) Show that there is a non-singular complete curve $\tilde{C}$ birationally isomorphic to C. In other words, there are rational maps $\phi: C\rightsquigarrow\tilde{C}$ and $\psi:\tilde{C}\rightsquigarrow C$ with $\phi\psi=\mathrm{id}$ and $\psi\phi=\mathrm{id}$. Show that any two such $\tilde{C}$ are isomorphic.

(b) If C is complete, then ψ is a surjective morphism.

(c) If C is non-singular, then ϕ is an injective morphism identifying C with an open set of the form $\tilde{C}\setminus\{P_1,...,P_n\}$.

Exc 4.2. Explain why Lemma 4.1 fails if one of the words ‘complete’, ‘non-singular’ or ‘curves’ is omitted.

Exc 4.3. Show that $\mathbb{P}^2$ and $\mathbb{P}^1\times\mathbb{P}^1$ have the same field of rational functions but are not isomorphic. (You may want to use Bezout’s theorem for $\mathbb{P}^2$.)

Exc 4.4. Prove that the complete variety in Nagata’s theorem (3.8) is not necessarily unique.

5. Differentials and genus

The main invariant of Riemann surfaces is the *genus*, and we now define it algebraically, over any k, in terms of differentials.

For any variety X/k, *rational k-differentials on X* are formal finite sums $\omega=\sum_i f_i dg_i$ with $f_i, g_i\in k(X)$, modulo the relations

$$d(f+g)=df+dg, \qquad d(fg)=fdg+gdf, \qquad da=0\ \ (a\in k).$$

If $k(X)$ is written as a finite separable extension[16] of a purely transcendental one $k(t_1,...,t_d)$, every differential has a unique expression $g_1dt_1+\ldots+g_ddt_d$ with $g_i\in k(X)$, and their space is $\cong k(X)^d$ as a k-vector space (Exc 5.1).

Example 5.1. $X=\mathbb{A}^n$ (or $\mathbb{P}^n$) has differentials $f_1dx_1+\ldots+f_ndx_n$ with $f_1,\ldots,f_n\in k(X)=k(x_1,...x_n)$.

Example 5.2. On the curve $C: y^2=x^3+1$ ($\operatorname{char} k\neq 2,3$) every differential can be written uniquely as $f(x,y)dx$, and also as $h(x,y)dy$ with $f,h\in k(C)$. (Use that $0=d(y^2-x^3-1)=2ydy-3x^2dx$ to transform between the two.)

A differential ω is *regular* at $P\in X$ if it has a representation $\omega=\sum_i f_idg_i$ with f_i,g_i regular at P.[17] If ω is regular everywhere, we call it a *regular differential*, and we write Ω_X for the k-vector space of those. For complete varieties $\dim_k\Omega_X$ is finite; if, moreover, X is projective and $k=\mathbb{C}$, regular differentials are the same as holomorphic differentials[18].

If ω is a rational differential on a curve, we can test whether it is regular at $P\in C$ as follows. Pick a uniformizer t at P, and write $\omega=f\,dt$ with $f\in k(C)$. Then ω is regular at P if and only if f is, that is $\operatorname{ord}_P f\geq 0$. Generally, we can define the order of vanishing of a (non-zero) differential:

Definition 5.3. If t is a uniformizer at P, we let $\operatorname{ord}_P(f\,dt)=\operatorname{ord}_P f$.

This means that we can define a *divisor* (ω) *of a differential form* ω. It is easy to see that all such divisors are linearly equivalent.

Definition 5.4. The *genus* g of a complete non-singular curve C is $\dim_k\Omega_C$. If C is any curve, its *geometric genus* is the genus of the (unique) complete non-singular curve birational to C.

Example 5.5. $\mathbb{P}^1$ has no non-zero regular differentials, so it has genus 0. To see this, cover $\mathbb{P}^1=\mathbb{A}^1_x\cup\mathbb{A}^1_y$ with $xy=1$. Then $x-a$ are uniformizers at $a\in\mathbb{A}^1_x$, so $dx=d(x-a)$ has no zeros or poles on $\mathbb{A}^1_x$, and similarly dy on $\mathbb{A}^1_y$. Now, a rational differential $\omega=f(x)dx\neq 0$ on the x-chart looks as follows on the y-chart:

$$0=d(xy-1)=xdy+ydx\qquad\Longrightarrow\qquad f(x)dx=-y^{\deg f-2}f(1/y)dy.$$

For ω to be regular everywhere, $f(x)$ must be a polynomial in x ($\Leftrightarrow$ regular on $\mathbb{A}^1_x$), and $y^{\deg f-2}f(1/y)$ a polynomial in y as well, and that is impossible. In fact, the computation shows that $\deg(\omega)=-2$ for every ω, so (ω) always has poles.

[16] So, if $\operatorname{char} k=0$, any algebraically independent $t_1,...,t_d\in k(X)$ will do ($d=\dim X$).

[17] If $P\in X$ is a non-singular point, there is an easy test: pick algebraically independent functions $g_1,...,g_d\in k(X)$ so that $g_i-g_i(P)$ generate m_P/m_P^2, and write $\omega=\sum_i f_idg_i$. Then ω is regular at P if and only if all the f_i are (Exc 5.2)

[18] These are special cases of finite-dimensionality of the space of global sections of a coherent sheaf on a complete variety, and of Serre's 'Géométrie Algébrique Géométrie Analytique' (GAGA) principle for complex projective varieties.

Example 5.6. The differential $\frac{dx}{y}$ on $y^2 = x^3 + 1 \subset \mathbb{P}^2$ ($\operatorname{char} k \neq 2, 3$) is regular everywhere (check this directly).

Generally, say $C : f(x, y) = 0$ is a non-singular affine curve. How do we find the genus of the corresponding complete curve, and the regular differentials? Take a point $P = (a, b)$ on C. The maximal ideal of $O = O_{C,P}$ is $m = (x-a, y-b)$ and (at least) one of these generators is a uniformizer. Explicitly, expand $f(x, y)$ at P,

$$f(x, y) = 0 + f'_x(P)(x - a) + f'_y(P)(y - b) + \text{ terms in } m^2.$$

We see that either

$$\begin{array}{ccc} f'_x(P) \neq 0,\ x-a \in (y-b)O + m^2 & \text{or} & f'_y(P) \neq 0,\ y-b \in (x-a)O + m^2. \\ \Downarrow & & \Downarrow \\ y-b \text{ uniformizer}, \operatorname{ord}_P \frac{dx}{f'_y} = 0 & & x-a \text{ uniformizer}, \operatorname{ord}_P \frac{dy}{f'_x} = 0. \end{array}$$

But

$$0 = df = f'_x\, dx + f'_y\, dy \qquad \Longrightarrow \qquad \frac{dx}{f'_y} = -\frac{dy}{f'_x},$$

so this differential has no zeroes or poles on C. Therefore $x^i y^j \frac{dx}{f'_y}$ have no poles on C either, and form a basis of such differentials. If we embed $\mathbb{A}^2$ as an open set of some complete variety[19], say X, the closure $\bar{C}$ of C in X is a complete curve. To check whether $\bar{C}$ is non-singular and to find its genus we just have to see what happens at the finitely many points $\bar{C} \setminus C$.

There is one general result that addresses the case when X is a toric variety[20]. It gives a formula for the so-called arithmetic genus of $\bar{C}$ in X, and that agrees with the genus of $\bar{C}$ if $\bar{C}$ happens to be non-singular (and gives an upper bound on it in general):

Theorem 5.7 (Baker). *Let $C : \sum_{i,j} c_{ij} x^i y^j = 0$ be a curve in $\mathbb{A}^2$, and $\bar{C}$ the unique non-singular complete curve birational to C. Write $\Delta \subset \mathbb{R}^2$ for the convex hull of points $(i, j) \in \mathbb{Z}^2$ for which $c_{ij} \neq 0$, and $I = (\Delta - \partial\Delta) \cap \mathbb{Z}^2$, the set of interior lattice points of Δ.*

1. *$\Omega_{\bar{C}}$ is contained in the k-vector space spanned by $x^{i-1} y^{j-1} \frac{dx}{f'_y}$ with $(i, j) \in I$. In particular, the genus of $\bar{C}$ is at most $|I|$.*
2. *The equality $\operatorname{genus}(\bar{C}) = |I|$ holds if and only if $C \subset \mathbb{A}^2$ is non-singular and certain conditions on the monomials in $\partial\Delta$ are satisfied.*[21]

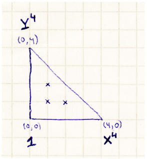
Proof. Over $\mathbb{C}$ this is a theorem of Baker [Bak] from 1893. See [KWZ] Prop. 3.3 and [BP] Thm 4.2 for the modern formulations and proofs. □

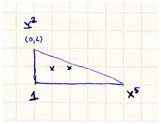
[19] Could be $\mathbb{P}^2$, $\mathbb{P}^1 \times \mathbb{P}^1$, weighted projective space, ...

[20] ...and toric varieties cover all the examples from the previous footnote

[21] E.g. if for all segments of the boundary $\sigma \subset \partial\Delta$, the polynomial $f_\sigma = \sum_{(i,j)\in\sigma} c_{ij} x^i y^j$ is squarefree

Example 5.8. If $\operatorname{char} k \neq 2, 5$, the curves $x^4 + y^4 = 1$ and $y^2 = x^5 + 1$ are non-singular, of genus 3 and 2, respectively.





Both examples generalise:

Example 5.9. (Plane curves) A curve given by a non-singular homogeneous equation $f = 0 \subset \mathbb{P}^2$ has genus $g = \frac{(d-1)(d-2)}{2}$, $d = \deg f$.[22]

Example 5.10 (Hyperelliptic curves, $\operatorname{char} k \neq 2$)**.** Let $f(x)$ be a polynomial of degree $2g+1$ or $2g+2$ with no multiple roots, for some $g \geq 0$. The two affine charts

$$y^2 = f(x) \qquad \text{and} \qquad Y^2 = X^{2g+2} f(\tfrac{1}{X})$$

glue via $Y = \frac{y}{x^{g+1}}$, $X = \frac{1}{x}$ to a complete, non-singular curve C. It has a map $C \to \mathbb{P}^1$ (via $(x, y) \mapsto x$), and such curves are called *hyperelliptic*. It has genus g, with regular differentials

$$\Omega_C = \Bigl\langle \frac{dx}{y}, \frac{xdx}{y}, \ldots, \frac{x^{g-1}dx}{y} \Bigr\rangle.$$

Conversely, any hyperelliptic curve has such a model (use $[k(C) \colon k(x)] = 2$).

Exc 5.1. Suppose X is an n-dimensional variety, $t_1, ..., t_n \in k(X)$ are algebraically independent and the (finite) extension $k(X)/k(t_1, ..., t_n)$ is separable (e.g. $\operatorname{char} k = 0$). Then every rational differential on X can be written uniquely as $g_1 dt_1 + \ldots + g_n dt_n$ with $g_i \in k(X)$.

Exc 5.2. Suppose X is a variety, $P \in X$ a non-singular point, and $g_1, ..., g_{\dim X} \in k(X)$ are algebraically independent functions so that $g_i - g_i(P)$ generate the k-vector space m_P/m_P^2. ($m_P \subset O_{X,P}$ is the maximal ideal.) Then $\omega = \sum_i f_i dg_i$ is regular at P if and only if all the f_i are.

Exc 5.3. Suppose $\operatorname{char} k \neq 2$. Let $C : y^2 = f(x)$ with $f(x) \in k[x]$ of degree $2g+1$ or $2g+2$ with no multiple roots. Prove that $\Omega_C = \langle \frac{dx}{y}, \frac{xdx}{y}, \ldots, \frac{x^{g-1}dx}{y} \rangle$.

6. Riemann-Roch

The most important result for curves (or compact Riemann surfaces) is the Riemann-Roch theorem, which we now recall.

[22] The conditions of Baker's theorem here are that the affine curve $f = 0$ is non-singular, and that the highest (degree d) part of f is square-free, i.e. the curve $\bar{C}$ meets the line at infinity $\mathbb{P}^1 = \mathbb{P}^2 \setminus \mathbb{A}^2$ in exactly n points. This is sufficient, though not a necessary condition for the completion of $f = 0$ in $\mathbb{P}^2$ to be non-singular.

Notation 6.1. For a divisor $D \in \operatorname{Div} C \setminus \{0\}$ on a non-singular complete curve, write

$$\mathcal{L}(D) \ = \ \{f \in k(C)^{\times} \,|\, \operatorname{div} f \geq -D\} \cup \{0\},$$

the space of functions with 'poles at worst at D'. Note that this space is 0 when $\deg D < 0$, and also that

$$(\mathcal{L}(D) \setminus \{0\})/k^{\times} \ \overset{1:1}{\longleftrightarrow} \ \{D' \geq 0 \,|\, D' \sim D\},$$

the set of effective divisors linearly equivalent to D.

We let

$$K_C = [\operatorname{div} \omega] \quad \in \operatorname{Div} C,$$

the class in $\operatorname{Pic} C$ of the divisor of any differential form ω on C, the *canonical divisor.* Note that $\dim \mathcal{L}(K_C) = \operatorname{genus}(C)$.

Theorem 6.2 (Riemann-Roch)**.** *Let C be a complete non-singular curve of genus g. For every divisor D on C,*

$$\dim \mathcal{L}(D) - \dim \mathcal{L}(K - D) = \deg D - g + 1.$$

Corollary 6.3.

(1) $\deg K_C = 2g - 2$.
(2) *If* $\deg D > 2g - 2$*, then* $\dim \mathcal{L}(D) = \deg D - g + 1$.

Proof. (1) Put $D = K_C$ in Riemann-Roch and use that $\mathcal{L}(0) = k$, as every non-constant function f on C has a pole (as $f : C \twoheadrightarrow \mathbb{P}^1$). (2) $\deg(K_C - D) < 0$, so $\mathcal{L}(K_C - D) = 0$. □

Example 6.4 (Genus 0)**.** If $g = 0$, and $D = (P)$ (a point), we get $\dim \mathcal{L}(D) = 2$, so $\mathcal{L}(D) = \langle 1, f \rangle$ for some non-constant $f \in k(C)^{\times}$. As f has one pole (at P) and one zero, it gives a degree 1 map $f : C \to \mathbb{P}^1$ which must be an isomorphism. So every genus 0 curve is isomorphic to $\mathbb{P}^1$.

Remark 6.5. This also shows that, conversely, on a curve C of positive genus, $(P) \not\sim (Q)$ for any $P \neq Q$ and so $\mathcal{L}((P)) = k$ for every $P \in C$.

Example 6.6 (Genus 1. Weierstrass form for elliptic curves)**.** A genus one curve C with a chosen point ('origin') $\mathcal{O} \in C$ is called an *elliptic curve.*

Suppose $(C, \mathcal{O})$ is such a curve. We have $\mathcal{L}(0) = \mathcal{L}(\mathcal{O}) = k$ (use Remark 6.5), and $\dim \mathcal{L}(n \cdot (\mathcal{O})) = n$ for $n > 1$. In particular,

$$\begin{aligned} \mathcal{L}(2 \cdot (\mathcal{O})) &= \langle 1, x \rangle, \\ \mathcal{L}(3 \cdot (\mathcal{O})) &= \langle 1, x, y \rangle \end{aligned}$$

for some $x, y \in k(C)^{\times}$, and x has exactly a double pole at $\mathcal{O}$ and no other poles, and y a triple pole at $\mathcal{O}$ and no other poles. Inspecting

$$\mathcal{L}(6 \cdot (\mathcal{O})) = \langle 1, x, y, x^2, xy, x^3, y^2 \rangle,$$

we see that this 7 functions in a 6-dimensional k-vector space must have a linear relation that involves x^3 and y^2, the two functions with a pole of order 6 at $\mathcal{O}$. Rescaling them if necessary, we may assume that the relation is of the form

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6, \qquad a_i\in k^\times. \tag{6.7}$$

Let C' be a curve given by this affine equation. As $[k(C):k(x)]=2$ (x has one double pole, and hence degree 2) and $[k(C):k(y)]=2$, we must have $[k(C):k(x,y)]=[k(C):k(C')]=1$, and so C is birational to C'. Moreover, C' must be non-singular, as otherwise it has geometric genus 0 by Theorem 5.7 and is birational to $\mathbb{P}^1$ (so $C\cong\mathbb{P}^1$ cannot have genus 1). Therefore $C\cong C'$, in other words every elliptic curve has an equation of the form (6.7), called a *Weierstrass equation.*

In characteristic $\neq 2,3$, we can complete the square on the left and cube on the right, so the equation becomes in *simplified Weierstrass form*,

$$y^2=x^3+Ax+B, \qquad \text{RHS squarefree}$$

Remark 6.8. Note also that the Weierstrass equation (6.7) is essentially unique for a given curve. The only functions with a double pole at $\mathcal{O}$ are $ax+b$ ($a\neq 0$) and with a triple pole $cy+dx+e$ ($c\neq 0$). So the only isomorphisms between elliptic curves in Weierstrass form are[23]

$$x\mapsto u^2x+r, \qquad y\mapsto u^3y+sx+t, \qquad u\in k^\times, r,s,t\in k.$$

and those between simplified Weierstrass equations

$$x\mapsto u^2x, \qquad y\mapsto u^3y+sx+t, \qquad u\in k^\times,$$

which as isomorphism

$$y^2=x^3+ax+b \qquad \xrightarrow{\cong} \qquad y^2=x^3+u^4ax+u^6b.$$

It is not hard to deduce from this, that an elliptic curve $(E,\mathcal{O})$ has ≤ 24 automorphisms, and ≤ 6 automorphisms in characteristic $\neq 2,3$ (Exc 6.1).

Example 6.9 (Genus 2)**.** A similar argument shows that every genus 2 curve has a model

$$y^2+f(x)y=g(x), \qquad \deg f\leq 3, \deg g\leq 6.$$

In characteristic $\neq 2$, we can write this as

$$y^2=g(x), \quad \deg g\in\{5,6\},$$

with g a square-free polynomial. See Exc 6.2.

Lecture 4

How to we classify curves of arbitrary genus, and give them explicit models? It is natural to try and embed curves into some projective spaces, and this is, in a way, equivalent to understanding the spaces $\mathcal{L}(D)$ for divisors D on C. If $D\in\mathrm{Div}^0(C)$ and $f_1,\ldots,f_n$ is a basis of $\mathcal{L}(D)\neq 0$, then

$$\phi: C\rightsquigarrow\mathbb{P}^{n-1}, \qquad P\mapsto[f_1(P):\ldots:f_n(P)]$$

[23] The coefficients u^2, u^3 come from our choice that y^2-x^3 has a pole of order <6.

is a rational map, and a different basis of $\mathcal{L}(D)$ only changes the map by a linear change of variables on $\mathbb{P}^n$, i.e. an automorphism in $\mathrm{PGL}_n(k)$. It also clearly depends only on the class of D in $\mathrm{Pic}^0(C)$. There are conditions to guarantee that ϕ is an *closed immersion* (isomorphism with a closed subvariety of $\mathbb{P}^{n-1}$)[24] and $\phi(C)$ in $\mathbb{P}^{n-1}$ whose *degree* (number of points in an intersection with a generic hyperplane) is the degree of D.

Example 6.10. For an elliptic curve $(C, \mathcal{O})$, take $D = \mathcal{L}(n \cdot (\mathcal{O}))$ for $n \geq 1$.

$$\begin{array}{lcll}
\mathcal{L}(1 \cdot (\mathcal{O})) & = & \langle 1 \rangle & \text{gives} \quad E \longrightarrow \mathbb{P}^0 = \{\mathrm{pt}\} \\
\mathcal{L}(2 \cdot (\mathcal{O})) & = & \langle 1, x \rangle & \text{gives} \quad E \xrightarrow{2:1} \mathbb{P}^1 \\
\mathcal{L}(3 \cdot (\mathcal{O})) & = & \langle 1, x, y \rangle & \text{gives} \quad E \xrightarrow{\cong} \text{cubic} \subset \mathbb{P}^2 \\
\mathcal{L}(4 \cdot (\mathcal{O})) & = & \langle 1, x, y, x^2 \rangle & \text{gives} \quad E \xrightarrow{\cong} \text{deg 4 curve} \subset \mathbb{P}^3 \\
\quad \cdots & & &
\end{array}$$

We know that this is a closed immersion for $n = 3$, and the same follows for $n > 3$. For example, for $n = 4$ the image (given by the relations between $1, x, y, x^2$ in $k(C)$) is the intersection of two quadrics in $\mathbb{P}^3$,

$$x_0 x_3 = x_1^2, \;\; x_2^2 = x_1 x_3 + A x_0 x_1 + B x_0^2 \qquad (\text{if } \; C : y^2 = x^3 + Ax + B).$$

The geometry of these curves become rather involved for high n.

When $\deg D$ is large, the dimension of $\mathcal{L}(D)$ is given by Riemann-Roch, and does not depend on the curve, but for small D this is not the case. Existence of such linear systems can be used naturally to classify curves[25], though a complete classification is certainly not known.

Example 6.11. The *canonical* map, given by the canonical divisor $D = K_C$,

$$\phi : C \mapsto \mathbb{P}^{g-1}, \qquad \phi(C) = \text{curve of degree } 2g - 2.$$

For non-hyperelliptic curves this is an embedding[26]. Otherwise, for $g \geq 3$,

$$C \;\xrightarrow{2:1}\; \mathbb{P}^1 \;\hookrightarrow\; \mathbb{P}^{g-1}.$$

Conversely, given a curve of degree $2g - 2$ in $\mathbb{P}^{g-1}$, intersecting it with a generic hyperplane cuts out an effective divisor in the canonical class.

Example 6.12.

- A *genus 3* curve is either hyperelliptic (y^2 =degree 7 or 8), or a quartic $\subset \mathbb{P}^2$ via the canonical embedding (and not both).
- A *genus 4* curve is either hyperelliptic (y^2 =degree 9 or 10), or quadric surface $\cap$ cubic surface $\subset \mathbb{P}^3$ via the canonical embedding.

[24] See [H]; in particular if it is a closed immersion for D, it is for any $D + (P)$ as well.

[25] And there are known restrictions. For instance, a theorem of Clifford [H, Thm. 5.4] that that an effective special divisor D (i.e. $D \geq 0$, $\dim \mathcal{L}(K - D) > 0$) on C has $\dim \mathcal{L}(D) \leq \frac{1}{2} \deg D$, and equality occurs if and only if either $D = 0$, $D \in [K_C]$, or C is hyperelliptic and D lies in a multiple of the unique effective divisor class of degree 2 on C.

[26] In particular, non-hyperelliptic curves are projective. For hyperelliptic curves this is true as well, so for curves 'complete' and 'projective' are the same thing.

- A *genus 5* curve is either hyperelliptic (y^2 =degree 11 or 12), or the intersection of three quadrics in $\mathbb{P}^4$ via the canonical embedding.

Starting from genus 6, canonically embedded curves are not complete intersections, and working with explicit models for them generally becomes complicated.

Exc 6.1. An elliptic curve $(E, \mathcal{O})$ has ≤ 24 automorphisms, and ≤ 6 automorphisms in characteristic $\neq 2, 3$.

Exc 6.2. Every genus 2 curve has a hexic (or even quintic) model.

Exc 6.3. A singular cubic is birational to $\mathbb{P}^1$ — prove directly.

7. Picard groups of curves

Riemann-Roch also gives a way to understand Picard groups of curves.

Example 7.1. On $C = \mathbb{P}^1$ any divisor $D = \sum\limits_{a \in \mathbb{P}^1} n_a(a)$ of degree 0 is principal,

$$D = (f), \qquad f = \prod_{a \neq \infty} (x-a)^{n_a}.$$

So $\operatorname{Pic}^0 \mathbb{P}^1 = \{0\}$ and $\operatorname{Pic} \mathbb{P}^1 = \mathbb{Z}$.

Example 7.2 (Genus 1)**.** On an elliptic curve $(E, \mathcal{O})$ every divisor of degree 0 is linearly equivalent to $(P) - (O)$ for a unique $P \in E$.

Indeed, if $D \in \operatorname{Div}^0(E)$, then $\mathcal{L}(D + (\mathcal{O}))$ is 1-dimensional by Riemann-Roch, so there is a function f with $(f) \geq -D - (\mathcal{O})$. Then $(f) = -D - (\mathcal{O}) + (P)$ for some $P \in E$, and $D \sim (P) - (\mathcal{O})$. Also, as f is unique up to scalars, such a point P is unique as well.

This shows that $P \mapsto (P) - (\mathcal{O})$ is a bijection $E \overset{1:1}{\leftrightarrow} \operatorname{Pic}^0 E$, and this makes E into an abelian group, with $\mathcal{O}$ as the origin! Geometrically, if E is in Weierstrass form with $\mathcal{O} = [0:1:0]$, the group is determined by

$$P + Q + R = 0 \qquad \Leftrightarrow \qquad P, Q, R \text{ lie on a line.}$$

Indeed, if L is the line through P and Q (and tangent to P if $P = Q$),

$$L : \alpha y + \beta x + \gamma = 0,$$

then the function $\alpha y + \beta x + \gamma$ has a triple pole at $\mathcal{O}$ and no other poles. So its divisor is

$$(\alpha y + \beta x + \gamma) = (P) + (Q) + (R) - 3(\mathcal{O}),$$

for a unique $R \in C$, and

$$(P) - (\mathcal{O}) + (Q) - (\mathcal{O}) + (R) - (\mathcal{O}) = 0 \quad \in \operatorname{Pic}^0(E).$$

To add two points P and Q we connect them with a line, find the third point of intersection R', and let $P + Q = R$ be the other point that has the same x-coordinate as R' (since $R = -R'$ — check).

It is not difficult to deduce from this, and this is a very important fact, that the group law on an elliptic curve is given by a *morphism* $E \times E \to E$.

So E is an algebraic group (not affine), and we will get to them in the next section.

Example 7.3 (Genus 2)**.** Let C be a complete non-singular curve of genus 2. Suppose $\operatorname{char} k \neq 2$ for simplicity, and put C in the form

$$C : y^2 = x^5 + a_4x^4 + \ldots + a_0 \qquad \text{squarefree.}$$

This particular model has a unique point ∞ at infinity (while $y^2 = \deg 6$ has 2). The curve is hyperelliptic, and we write i for the *hyperelliptic involution* $(x, y) \mapsto (x, -y)$. (This is the map for which i^* generates $\mathrm{Gal}(k(C)/k(x))$.)

Recall that $\Omega_C = \langle \frac{dx}{y}, \frac{xdx}{y} \rangle$, and compute their divisors

$$(\tfrac{dx}{y}) = 2(\infty), \quad (\tfrac{(x-a)dx}{y}) = (P_a) + (i(P_a)), \quad P_a = (a, \sqrt{f(a)}).$$

So the divisors in the canonical class are the fibers of $C \to \mathbb{P}^1$. By Riemann-Roch, every other divisor class of degree 2 has a unique effective divisor. Therefore, as a set, $\mathrm{Pic}^2 C$ (divisors of degree two modulo $\sim$) is the set of unordered pairs $\{P, P'\}$ of points in C, except that all elements of the form $\{P, i(P)\}$ are identified with each other.

Under the identification of $\mathrm{Pic}^0 C$ with $\mathrm{Pic}^2 C$ by adding K, the group law on $\mathrm{Pic}^0 C$ is generically as follows. The inverse map is

$$(P) + (P') \longmapsto (i(P)) + (i(P')).$$

To add $D_1 = (P) + (P')$ with $D_2 = (Q) + (Q')$, find a unique curve

$$y = a_0x^3 + a_1x^2 + a_2x + a_3$$

passing through $\{P, P', Q, Q'\}$. It intersects the curve in two other points R, R', and letting $D_3 = R + R'$ we have $D_1 + D_2 + D_3 \sim 0$. In other words, $D_1 + D_2 = i(D_3)$.

Remark 7.4. Generally, on a curve C of any genus $g > 0$, every degree g divisor is equivalent to one of the form $P_1 + \ldots + P_g$, and this representation is 'usually' (in the Zariski open-sense) unique. A nice example (Cantor [Can]), is that when $\operatorname{char} k \neq 2$, on a hyperelliptic curve

$$y^2 = x^{2g+1} + a_{2g}x^{2g} + \ldots + a_1x + a_0 \qquad =: f(x),$$

every class in $\mathrm{Pic}^0 C$ is represented by a unique divisor $(P_1) + \ldots + (P_r) - r(\infty)$ with $r \leq g$ and P_i affine points with $P_j \neq i(P_i)$ for $j \neq i$.

For example, in this case, the *2-torsion* points $D \in \mathrm{Pic}^0(C)$ (those with $2D = 0$, equivalently $D \sim i(D)$) are represented by

$$(\alpha_1, 0) + \ldots + (\alpha_r, 0) - r(\infty), \qquad 0 \leq r \leq g,\ \alpha_i \text{ distinct},\ f(\alpha_i) = 0.$$

There are $\binom{2g+1}{g} + \binom{2g+1}{g-1} + \ldots + \binom{2g+1}{0} = 2^{2g}$ of these in total, and they form a $\mathbb{F}_2$-vector space $\cong \mathbb{F}_2^{2g}$.

Remark 7.5. In general, $\mathrm{Pic}^0(C)$ has a structure of an g-dimensional *algebraic group*, which is an *abelian variety.* We get to these now.

8. General algebraic groups

As before, $k = \bar{k}$ is an algebraically closed base field. We define algebraic groups from varieties exactly as in the affine case (Def. 2.1).

Definition 8.1. A group G is an *algebraic group* if it has a structure of an algebraic set, and multiplication $G \times G \to G$ and inverse $G \to G$ are morphisms.

As before, *homomorphisms* refer to morphisms that are group homomorphisms, *isomorphisms* are isomorphisms of both groups and varieties, and *subgroups* and *normal subgroups* always refer to closed ones.

Example 8.2. Affine algebraic groups $\mathbb{G}_m, \mathbb{G}_a, \mathrm{GL}_n, \ldots$ are algebraic groups.

Example 8.3. Elliptic curves and their products are algebraic groups.

Example 8.4. The multiplication-by-m map $[m] : G \to G$ is a homomorphism for any commutative algebraic group G and $m \in \mathbb{Z}$ (Exc 8.1).

Basic properties of algebraic groups carry over immediately from the affine case: an algebraic group G is a semidirect product $G = G^0 \rtimes \Delta$ of its connected component of identity G^0 and a finite discrete group Δ. Again, G^0 is a non-singular variety. Kernels and images of algebraic group homomorphisms exist, and so do factor groups in the same 'naïve' sense as before.

Example 8.5. Algebraic groups often occur naturally as automorphism groups of varieties (see Exc 8.2 though). For example, suppose C is a complete non-singular curve of genus g.

$(g = 0)$ $C \cong \mathbb{P}^1$, and $\operatorname{Aut} C \cong \mathrm{PGL}_2 = \mathrm{GL}_2 / \mathbb{G}_m$ is a Möbius group (Exc 8.3).
$(g = 1)$ Choosing a point $O \in C$ makes C into an elliptic curve, and $\operatorname{Aut} C \cong C \ltimes \operatorname{Aut}(C, O)$ with $\operatorname{Aut}(C, O)$ finite of order ≤ 24 (usually $\{\mathrm{id}, [-1]\}$.)
$(g \geq 2)$ $\operatorname{Aut} C$ is finite.[27]

Proposition 8.6. *The only one-dimensional connected algebraic groups are* $\mathbb{G}_a$*,* $\mathbb{G}_m$ *and elliptic curves.*

Proof. Write $G = C \setminus \{P_1, \ldots, P_n\}$ with C a non-singular complete curve (Exc 4.1), and take $x \in G$. The left translation map $l_x : y \mapsto xy$ on G extends to an automorphism

$$l_x : C \longrightarrow C,$$

because C is non-singular and complete. So C has infinitely many automorphisms that are (a) fixed point free on G, and (b) preserve the set of 'missing points' $\{P_1, \ldots, P_n\}$.

Write g for the genus of C, and $e \in G$ for the identity element.

[27] Hurwitz (1893) showed that $|\operatorname{Aut}(C)| \leq 84(g-1)$ over $\mathbb{C}$, and the bound is sharp for infinitely many g (Macbeath 1961). Schmid (1938) proved finiteness when $\operatorname{char} k = p > 0$ and noted that Hurwitz' bound fails for small p. It still holds when $p > g + 1$, except for $y^p - y = x^2$ which has $g = \frac{p-1}{2}$ and $|\operatorname{Aut}(C)| = 8g(g+1)(2g+1)$ (Roquette 1970).

$g \geq 2$: $\operatorname{Aut} C$ is finite, so this is impossible.

$g = 1$: If $n \geq 1$ then $|\operatorname{Aut}(C, P_1)| \leq 24$, so $n = 0$ and G is complete. For $x \in G$ there is a unique fixed point free map taking the identity element e to x, which must be l_x in every group law on G which has e as the identity element. So the group law must be the same one as the standard one on an elliptic one.

$g = 0$: Now $C \cong \mathbb{P}_1$ and $\operatorname{Aut} C \cong \mathrm{PGL}_2(k)$ is the group of Möbius transformations. These are uniquely determined by what they do to 3 given points, in particular $\operatorname{Aut} G \neq \{1\}$ implies $n \leq 2$.

$n = 0$: Then $l_x : \mathbb{P}^1 \to \mathbb{P}^1$ has no fixed points, which is impossible.

$n = 1$: Change the coordinate on $\mathbb{P}^1$ to move P_1 to ∞ and e to 0. The fixed point free automorphisms of $\mathbb{P}^1 - \{\infty\}$ are translations

$$z \mapsto z + a,$$

again there is a unique one taking 0 to a given $a \in G$, and $G = \mathbb{G}_a$.

$n = 2$: Similarly, move $P_1 \mapsto 0, P_2 \mapsto \infty$ and $e \mapsto 1$. The automorphisms of $\mathbb{P}^1 \backslash \{0, \infty\}$ are $z \mapsto az$ and $z \mapsto a/z$. Only the former ones are fixed point free, and there is a unique one taking $e \to x$ for a given x. So the group law is unique, $G = \mathbb{G}_m$. □

Lecture 5

Suppose G is an algebraic group over k. Recall that if G is an affine variety, G is also called a *linear algebraic group*.

Definition 8.7. An *abelian variety* is a complete connected algebraic group.

We have seen that 1-dimensional algebraic groups are either linear ($\mathbb{G}_a$, $\mathbb{G}_m$) or abelian varieties (elliptic curves). Much more generally, these two extremes build *all* algebraic groups:

Theorem 8.8 (Barsotti-Chevalley)**.** *Every connected algebraic group G fits into an exact sequence*

$$1 \longrightarrow H \longrightarrow G \longrightarrow A \longrightarrow 1$$

with $H \triangleleft G$ the unique largest linear connected subgroup of G, and A an abelian variety.

Remark 8.9. With the theory of linear groups thrown in, the classification can be extended. There is a unique filtration of G of the form

$$\begin{tikzcd}
G \arrow[r, dash, "\text{finite}"] & G_0 \arrow[r, dash, "\text{AV}"] & G_1 \arrow[r, dash, "\text{semisimple}"] & G_2 \arrow[r, dash, "\text{torus}"] & G_3 \arrow[r, dash] & 1 \\
 & \text{connected} & \text{linear} & \text{solvable} & \text{unipotent} &
\end{tikzcd}$$

with G_i connected and normal in G_{i-1}. Here:
A *torus* is an algebraic group isomorphic to $\mathbb{G}_m \times \cdots \times \mathbb{G}_m$;
A *unipotent group* is a subgroup of upper-triangular matrices with ones on the diagonal;
A *solvable group* is one admitting a filtration $1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_k = G$ with H_i/H_{i-1} commutative;

A *semisimple* group is one whose *radical* G_2 (the unique maximal connected linear solvable normal subgroup) is trivial; a semisimple group admits a finite covering $\mathcal{G}_1 \times \cdots \times \mathcal{G}_n \to G$ with $\mathcal{G}_i$ *almost simple* (finite centre C and $\mathcal{G}/C$ simple). Every almost simple group is isomorphic to either SL_{n+1} (type A_n), Sp_{2n} (type C_n), E_6, E_7, E_8, F_4, G_2 (exceptional groups) or isogenous to an orthogonal group (types B_n, D_n).

See [**?**] Ch. X for a more extended summary and references.

Example 8.10. $G = \mathrm{GL}_n$. Then $G = G_1$, $G_2 = Z(G) = \mathbb{G}_m$ and $G/G_2 = \mathrm{PGL}_n$ is simple.

Example 8.11. In characteristic 0, every connected *commutative* linear group is $U \cong (\mathbb{G}_m)^m \times (\mathbb{G}_a)^n$, and every commutative connected algebraic group G is an extension of an abelian variety A by a U as above, with A acting trivially on U.

Exc 8.1. Prove that the multiplication-by-m map $[m] : G \to G$ is a homomorphism for any commutative algebraic group G and $m \in \mathbb{Z}$.

Exc 8.2. Give an example of a variety V such that $\mathrm{Aut}\,V$ has no natural structure of an algebraic group.

Exc 8.3. Show that every automorphism of $\mathbb{P}^1_k$ is of the form $t \mapsto \frac{at+b}{ct+d}$. Deduce that $\mathrm{Aut}\,\mathbb{P}^1 \cong \mathrm{PGL}_2(k)$ $(= \mathrm{GL}_2(k)/k^*)$.

Exc 8.4. Show that there are no non-constant algebraic group homomorphisms from an abelian variety to a linear algebraic group.

9. Abelian varieties

Suppose $k = \bar{k}$ as before. Recall that an abelian variety A/k is an algebraic group over k, which is a complete variety. Let us validate 'abelian' and prove that abelian varieties are always commutative. This must clearly rely on completeness, and we follow Mumford's approach using rigidity:

Lemma 9.1 (Rigidity). *Suppose $f : V \times W \to U$ is a map of varieties, V is complete, and*

$$f(\{v_0\} \times W) = f(V \times \{w_0\}) = \{u_0\}$$

for some points v_0, w_0 and u_0. Then f is constant, $f(V \times W) = \{u_0\}$.

Proof.[28] Let U_0 be an open affine neighbourhood of u_0 and $Z = f^{-1}(U - U_0)$. This is a closed set, and so is its image under the projection $p_2 : V \times W \to W$, as V is complete.

As $w_0 \notin p_2(Z)$, the complement $W_0 = W - p_2(Z)$ is open dense in W. But for all $w \in W_0$ the image $f(V \times \{w\}) \subset U_0$ must be a point, as $V \times \{w\}$

[28] Over $k = \mathbb{C}$, this works as follows: if w is close to w_0, then $f(V \times \{w\})$ is close to u_0, by the compactness of V and continuity of f. So $f(V \times \{w\})$ is contained in some open ball around u_0. But there are no non-constant analytic maps from V to an open ball (maximum principle), so $f(V \times \{w\})$ is a point for such w, namely $f((v_0, w)) = u_0$. This proves that the set of such w is open; but it is also closed, so f is constant.

is complete and U_0 is affine. In other words, $f(V \times \{w\}) = f((v_0, w)) = u_0$. So $f^{-1}(u_0)$ contains a dense open $V \times W_0$; as $f^{-1}(u_0)$ is also closed, it must be the whole space, so f is constant. □

Corollary 9.2. *If U, V, W are varieties, V is complete, U is an algebraic group, and $f_1, f_2 : V \times W \to U$ are morphisms that agree on $\{v_0\} \times W$ and on $V \times \{w_0\}$, then they agree everywhere.*

Proof. The map $x \mapsto f_1(x)f_2(x)^{-1}$ is constant by the rigidity lemma. □

Corollary 9.3. *Abelian varieties are commutative.*

Proof. The maps xy and yx from $X \times X$ to X agree on $X \times \{e\}$ and $e \times X$, so they must agree everywhere by the previous corollary. □

Corollary 9.4. *Let $f : A \to B$ be a morphism of varieties between an abelian variety A and an algebraic group B.*

(1) *If f takes e to e, then f is a homomorphism of algebraic groups.*
(2) *In general, f is a composition of a translation on B and a homomorphism $A \to B$.*

Proof. (1) The morphisms $f(x) + f(y)$ and $f(x + y)$ from $A \times A$ to B agree on $\{0\} \times A$ and on $A \times \{0\}$, so they are equal. (2) Clear. □

Rigidity has another curious consequence: in defining an abelian variety we could have dropped the associativity condition, as it also follows automatically from rigidity! (Exc 9.1) For instance, for elliptic curves this gives a quick proof of the associativity of the group law, that only relies on E being complete.

Remark 9.5. It is possible to extend Corollary 9.4 slightly: any rational map $\phi : G \rightsquigarrow A$ from a connected algebraic group to an abelian variety is a composition of a translation with a homomorphism $G \to A$ (in particular, ϕ a morphism).

We will write the group operation on abelian varieties as addition, and denote the identity element by 0.

Exc 9.1. Suppose V is a complete variety, $e \in V(k)$ a point, and we have a morphism $* : V \times V \to V$ and an isomorphism $i : V \to V$. If $x*e = e*x = x$ and $x*i(x) = i(x)*x = e$, then $*$ is associative, so V is an abelian variety.

Exc 9.2. Prove that for an abelian variety A, every rational map $\mathbb{P}^1 \rightsquigarrow A$ is a constant morphism (hint: 9.5). Deduce that every rational map $\mathbb{P}^n \rightsquigarrow A$ is also constant.

Chapter 2. Families and moduli spaces

Perhaps THE most powerful technique in modern algebraic geometry is viewing a morphism $X \to Y$ as a family of varieties (fibres) parametrised by Y. For example,

$$\mathcal{E} : y^2 = x^3 + t^3 \qquad \subset \mathbb{A}^3$$

may be viewed either as a surface in $\mathbb{A}^3$ or as a family of curves $\mathcal{E}_t \subset \mathbb{A}^2_{x,y}$ parametrised by $t \in \mathbb{A}^1$. It is (an affine version of) 'an elliptic curve over $k[t]$', and if we embed $k[t]$ inside an algebraically closed field,

$$k[t] \subset k(t) \subset \overline{k(t)},$$

it becomes an elliptic curve as we know them. This allows us to pass between geometry of elliptic curves over one field and the geometry of surfaces (an 'elliptic surface' in this example) over another field. Some of the primary results of 20th century algebraic geometry[29] are proved by reducing questions about arbitrary varieties to those about curves, but over a general base.

Technically, working over general rings is best in the context of schemes, but the basics can be done without that. We review varieties over non-algebraically closed fields, then talk about families, and then introduce moduli spaces.

10. Varieties over any field

Suppose K is any field, and write $\bar{K}$ $(=k)$ for its algebraic closure.

Definition 10.1. If $V/\bar{K}$ is an affine variety that can be defined by polynomials with coefficients in K, we call it an *affine variety* V *over* K, denoted V/K. For such V, V', a *K-morphism* $V \to V'$ is a morphism that can be given by polynomials with coefficients in K. The *ring of regular functions on* $K[V]$ is the set of K-morphisms $V \to \mathbb{A}^1_K$.

If $L \supset K$ is a field, we write $V \times_K L$ or V_L for the same variety considered over L, and we call it V *base changed to* L. Its ring of regular functions is $K[V] \otimes_K L \subset \bar{K}[V]$, so it is an integral domain for any L. We say V is *regular* (*complete*, *of dimension* n, etc.) if $V \times_K \bar{K}$ is.[30]

The old definition of affine varieties, 'Zariski closed irreducible subset of K^n', does not work for non-algebraically closed fields. (E.g., if K is finite, the only varieties would be points!) The above one does work well, and $V \mapsto K[V]$ defines an equivalence of categories between affine varieties over K and finitely generated K-algebras A such that $A \otimes_k \bar{K}$ is an integral domain. We define a general *variety over* K similarly, as a variety over $\bar{K}$ covered by affine open subvarieties defined over K, and with transition

[29] e.g. Deligne's proof of the Weil conjecturs and de Jong's alterations

[30] Algebraic geometers say that V is 'geometrically whatever' if $V \times_K \bar{K}$ is 'whatever'. So our varieties are 'geometrically integral', regularity is 'geometric regularity' etc.

maps between them defined over K, and an *algebraic set over* K by dropping the irreducibility condition. As before, products $V \times W$ exist in all these categories, and

$$K[V \times W] = K[V] \otimes_k K[W].$$

Example 10.2. $\mathbb{A}^n$ and $\mathbb{P}^n$ are varieties that can be defined over any K.

Example 10.3. The line $C : \sqrt{2}x+\sqrt{3}y = 0 \subset \mathbb{A}^2$ is defined over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. It can be even defined over $\mathbb{Q}(\sqrt{6})$, because the ideal

$$(\sqrt{2}x + \sqrt{3}y)\bar{\mathbb{Q}}[x, y] \subset \bar{\mathbb{Q}}[x, y]$$

is generated by $x+\frac{\sqrt{6}}{2}y$. The curve is not defined over $\mathbb{Q}$ though (Exc 10.1).

Example 10.4. The equation $f : x^2+y^2=0$ in $\mathbb{A}^2$ does not define a variety over $\mathbb{R}$, as it is reducible over $\mathbb{C}$. In other words, although, $A = \mathbb{R}[x, y]/(x^2+y^2)$ is an integral domain, $A \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[x, y]/(x + iy)(x - iy)$ is not.

For simplicity, assume for the rest of this section that the ground field K is perfect, that is every finite extension of it is separable.

Definition 10.5. If V/K is an affine algebraic set, its *set of (K-)rational points* is

$$V(K) = V \cap K^n.$$

For a general V covered by affine charts V_i/K, we let $V(K) = \cup V_i(K)$.

Definition 10.6. For a curve C/K, we say that a divisor $D \in \mathrm{Div}(C)$ is *defined over* K if it is invariant under all automorphisms $\sigma \in \mathrm{Gal}(\bar{K}/K)$. (E.g. on $\mathbb{P}^1_{\mathbb{Q}}$, the divisors (0), $3(\infty)$, and $(2 + i) + (2 - i)$ are rational.)

Two complications when working over non-algebraically closed fields is that non-isomorphic varieties over K may become isomorphic over $\bar{K}$, and that varieties may not have any K-rational points, or even K-rational divisors of certain degrees.

Example 10.7 (Selmer)**.** The following plane curve $C/\mathbb{Q}$ of genus 1

$$C : \ 3x^3 + 4y^3 = 5z^3 \quad \subset \mathbb{P}^2_{\mathbb{Q}}$$

is isomorphic over $\bar{\mathbb{Q}}$ to the elliptic curve

$$E : y^2 = x^3 - 100/3.$$

However $C(\mathbb{Q}) = \emptyset$, so it is not an elliptic curve over $\mathbb{Q}$. In fact, all $\mathbb{Q}$-rational divisors on C have degree multiple of 3, so $C/\mathbb{Q}$ does not even admit a degree 2 map to $\mathbb{P}^1$.

Definition 10.8. An *elliptic curve* over K is a pair $(C, \mathcal{O})$, with C/K a curve of genus 1 and $\mathcal{O}$ is a K-rational point on C.

Fortunately, if a curve C has a K-rational divisor D, then $\mathcal{L}(D)$ has a basis of K-rational functions, so the associated map to $\mathbb{P}^n$ is defined over K:

Lemma 10.9. *Let V be a $\bar{K}$-vector space, and suppose that* $\mathrm{Gal}(\bar{K}/K)$ *acts continuously on V in a manner compatible with its action on $\bar{K}$. Then V has a basis of* $\mathrm{Gal}(\bar{K}/K)$*-invariant vectors.*

Proof. [Sil1] Lemma II.5.8.1. □

For example, if E/K is an elliptic curve, then we can apply the lemma to $\mathcal{L}(n \cdot \mathcal{O})$ for $n = 2, 3, ...$ to prove that E is isomorphic, over K, to an elliptic curve in Weierstrass form, exactly as before.

Example 10.10 (Genus 0)**.** Suppose C/K has genus 0. The divisor $D = (\omega)$ of any K-rational differential form $\omega \neq 0$ is K-rational, of degree -2. By Riemann-Roch, $\mathcal{L}(-D)$ is 3-dimensional and gives a map

$$C \to \mathbb{P}^2,$$

whose image is of degree 2, a conic (possibly singular). It is not hard to deduce that every genus 0 curve is isomorphic either to $\mathbb{P}^1_K$, or to a non-singular conic in $\mathbb{P}^2$,

$$f(x, y, z) = 0 \subset \mathbb{P}^2_K, \qquad \deg f = 2.$$

For instance, over $\mathbb{R}$, every curve of genus 0 is isomorphic to

$$\mathbb{P}^1_{\mathbb{R}} \qquad \text{or} \qquad x^2 + y^2 = -z^2 \subset \mathbb{P}^2,$$

and the latter has (visibly) no real points.

Example 10.11 (Genus 2, $\mathrm{char}\, K \neq 2$)**.** For a genus 2 curve C/K, the canonical divisor class has degree 2, and has again K-rational divisors in it. So as before, C has a model $y^2 = f(x)$ with $\deg f \in \{5, 6\}$.

Example 10.12 (Genus 1)**.** The canonical divisor class is 0, so we cannot infer the existence of a K-rational divisor of any specific degree. In other words, the degrees of K-rational divisors (clearly) form a non-zero subgroup $n\mathbb{Z}$ of $\mathbb{Z}$, and it is not clear whether there are any restrictions on n. In fact, over $\mathbb{Q}$, it is expected that all $n \geq 1$ can occur.

Lecture 6

These examples also illustrate the other aforementioned problem, having non-isomorphic varieties V, V' over K that become isomorphic over $\bar{K}$. Such varieties are called *forms* or *twists* of each other. Same terminology is used for algebraic groups G, G' over K that become isomorphic over $\bar{K}$, as algebraic groups.

In either setting, if V, V' are such twists, pick an isomorphism

$$i : V/\bar{K} \longrightarrow V'/\bar{K}.$$

Any automorphism $\sigma \in \mathrm{Gal}(\bar{K}/K)$ defines another such isomorphism i^σ, by acting on the coefficients of i, and the composition

$$\begin{array}{cccc} \xi : & \mathrm{Gal}(\bar{K}/K) & \longrightarrow & \mathrm{Aut}(V/\bar{K}) \\ & \sigma & \longmapsto & (i^\sigma)^{-1} i \end{array}$$

satisfies $\xi(\sigma\tau) = \xi(\sigma)^\tau \xi(\tau)$, which makes it into a 1-cocycle.

Theorem 10.13. *If either*

- *V is an algebraic group, or*
- *V is a quasi-projective variety (open subset of a projective variety) and $\mathrm{Aut}(V/\bar{K})$ is an algebraic group,*

then the above association gives a bijection

$$\textit{twists of } V \textit{ over } K \quad \overset{1:1}{\longleftrightarrow} \quad H^1(\mathrm{Gal}(\bar{K}/K), \mathrm{Aut}(V/\bar{K})).$$

Moreover, for a Galois extension L/K, twists of K that become isomorphic over L are in bijection with elements of $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(V/L))$.[31]

Example 10.14 (Elliptic curves)**.** Suppose $\mathrm{char}\, K \neq 2, 3$. An elliptic curve E/K has a Weierstrass equation

$$y^2 = x^3 + Ax + B,$$

and we call

$$dy^2 = x^3 + Ax + B \qquad (\cong y^2 = x^3 + d^2Ax + d^3B)$$

the quadratic twist of E by $d \in K^\times$. If $AB \neq 0$, then $\mathrm{Aut}_{\bar{K}}(E) = \{\pm 1\}$ with trivial Galois action, so

$$H^1(\mathrm{Gal}(\bar{K}/K), \mathrm{Aut}(E/\bar{K})) = \mathrm{Hom}(\mathrm{Gal}(\bar{K}/K), \{\pm 1\}).$$

A non-trivial element κ of this Hom is characterised by its kernel, the Galois group of some quadratic extension $K(\sqrt{d})$ of K. It correspond exactly to the quadratic twist E_d of E by d. Indeed, the map $i : E \to E_d$ given by $(x, y) \mapsto (x, \sqrt{d}y)$ is an isomorphism over $K(\sqrt{d})$, and

$$(i^\sigma){-}1i: \quad P = (x, y) \mapsto (x, y/\sqrt{d}) \mapsto (x, \tfrac{\sigma(\sqrt{d})}{\sqrt{d}} y) = \begin{cases} -P, & \sigma(\sqrt{d}){=}{-}\sqrt{d} \\ P, & \sigma(\sqrt{d}){=}\sqrt{d} \end{cases}$$

is the corresponding cocycle in $\mathrm{Hom}(\mathrm{Gal}(\bar{K}/K), \{\pm 1\})$.

Finally, there are two exceptional curves with more automorphisms

$$\begin{array}{ll} E : y^2 = x^3 + x & \qquad \mathrm{Aut}(E/\bar{K}) \cong \langle \zeta_4 \rangle \\ E : y^2 = x^3 + 1 & \qquad \mathrm{Aut}(E/\bar{K}) \cong \langle \zeta_6 \rangle. \end{array}$$

In this case we the corresponding twists are

$$\begin{array}{lll} E : y^2 = x^3 + dx & \qquad d \in K^\times/K^{\times 4} & \text{(quartic twists)} \\ E : y^2 = x^3 + d & \qquad d \in K^\times/K^{\times 6} & \text{(sextic twists).} \end{array}$$

(In characteristic 2 and 3, there are curves with even more automorphisms, and they have, correspondingly, other twists.)

Exc 10.1. Show that $C : \sqrt{2}x + \sqrt{3}y = 0$ in $\mathbb{A}^2_{\bar{\mathbb{Q}}}$ is not defined over $\mathbb{Q}$.

Exc 10.2. Show that the unit quaternions ($x_1 + x_2 i + x_3 j + x_4 k$ with $\sum x_i^2 = 1$) give an algebraic over $\mathbb{R}$, which is a form of $\mathrm{SL}_2(\mathbb{R})$

[31] These H^1's are pointed sets, and they are groups if Aut is abelian

11. Examples of moduli problems

There are many classification problems in algebraic geometry in which objects that we wish to classify are naturally in one-to-one correspondence with points on some variety X, called the *moduli space* for that problem. Postponing for the moment what 'naturally' means, here are a few examples, starting with the classification of subvarieties in a fixed ambient space.

As before, let us work over a fixed algebraically closed field k.

Example 11.1. *Lines through the origin in* $\mathbb{A}^2$ are parametrised by points of $\mathbb{P}^1$, which has a structure of an algebraic variety[32]:

$$ax + by = 0 \qquad \longleftrightarrow \qquad [a : b] \in \mathbb{P}^1_k.$$

Similarly, all lines $ax + by + c = 0$ in $\mathbb{A}^2$ are parametrised by $\mathbb{P}^2 \setminus \{[0 : 0 : 1]\}$ (and lines in $\mathbb{P}^2$ by $\mathbb{P}^2$, the missing point being the unique line at infinity).

Example 11.2. *Curves of degree 2 in* $\mathbb{P}^2$ *(conics)* have equations

$$a_0x^2 + a_1xy + a_2xz + a_3y^2 + a_4yz + a_5z^2 = 0,$$

and, again, (a_i) and $\lambda(a_i)$ define the same conic. So they are parametrised by points of $\mathbb{P}^5$, except that some points that define reducible conics have to be thrown away. If

$$a_0x^2+a_1xy+a_2xz+a_3y^2+a_4yz+a_5z^2 = (b_0x+b_1y+b_2z)(c_0x+c_1y+c_2z),$$

then (a_i) is in the image Z of the map $\mathbb{P}^2 \times \mathbb{P}^2 \to \mathbb{P}^5$ obtained by equating the components[33]. As Z is closed (image of a complete variety under a morphism), its completement has a structure of a variety, and

$$\{\text{conics in } \mathbb{P}^2\} \overset{1:1}{\longleftrightarrow} \mathbb{P}^5 \setminus Z.$$

(In such situations, we say that 'being irreducible is an open condition'.)

Another problem, perhaps a more natural one, is classifying varieties up to isomorphism. There are usually discrete invariants (like the dimension or the genus) which split the problem into 'connected components', and fixing them leads to a set that may have, again, a structure of a variety.

Example 11.3. *Genus 0 curves* over k are all isomorphic to $\mathbb{P}^1$, so the variety parametrising them is a point.

Example 11.4. All *genus 1 curves* C or *elliptic curves* $(E, \mathcal{O})$[34], say in characteristic $\neq 2, 3$, can be given by Weierstrass equations

$$y^2 = x^3 + Ax + B \qquad (\cong \;\; y^2 = x^3+Au^4\,x+Bu^6, \;\; u \in k^\times).$$

[32] Generally, d-dimensional linear subspaces of $\mathbb{A}^n$ are again parametrised by a variety, called the Grassmanian $\mathrm{Gr}(d, \mathbb{A}^n)$.

[33] $[b_0 : b_1 : b_2], [c_0 : c_1, c_2] \mapsto [b_0c_0 : b_0c_1{+}b_1c_0 : b_0c_2{+}b_2c_0 : b_1c_1 : b_1c_2{+}b_2c_1 : b_2c_2]$

[34] For this example it does not matter, as $(E, \mathcal{O}_1) \cong (E, \mathcal{O}_2)$ via a translation map.

The j-invariant (the constant 1728 is there for arithmetic reasons)

$$j(E)=1728\frac{4A^3}{4A^3+27B^2} \qquad \in k$$

is unchanged under isomorphisms of Weierstrass equations, and so is really an invariant of an isomorphism class of genus 1 curves. Moreover, $j(E)=j(E')$ implies $E\cong E'$ (Exc 11.1). Conversely, every $j\in k$ is the j-invariant of some curve, e.g.

$$E_j: y^2+xy=x^3-\frac{36}{j-1728}x-\frac{1}{j-1728} \qquad (j\neq 0,1728),$$

and two curves not covered by this formula,

$$E_0: y^2=x^3+1, \qquad E_{1728}: y^2=x^3+x.$$

In other words, genus 1 curves over k up to isomorphism are parametrised by points of $k=\mathbb{A}^1$ (the *j-line*), via the j-invariant map.

Generally, we can consider the set $M_{g,n}$ of isomorphism classes of curves C/k of genus g with n distinct marked points $P_1,...,P_n\in C$. The points are *ordered*, so an isomorphism $(C,(P_i))\to(C',(P'_i))$ is an isomorphism $C\to C'$ that takes P_i to P'_i.

If we make the points *unordered* instead, we get the set $M^{\text{sym}}_{g,n}=M_{g,n}/S_n$, where the symmetric group S_n acts naturally, permuting the marked points.

Example 11.5 (Genus 0)**.** Since every curve of genus 0 is isomorphic to $\mathbb{P}^1$, and $\text{Aut}(P^1)$ is the Möbius group that acts triply transitively on points,

$$M_{0,0}=M_{0,1}=M_{0,2}=M_{0,3}=\{\text{pt}\}.$$

For higher n, every $(C,(P_i))\in M_{0,n}$ is represented by a unique curve

$$(\mathbb{P}^1,(0,1,\infty,P_4,...,P_n)),$$

and so we have a natural identification

$$M_{0,n}=\Bigl(\mathbb{P}^1\setminus\{0,1,\infty\}\Bigr)^{n-3}\setminus\{\text{diagonals } x_i=x_j\}.$$

Example 11.6 (Genus 1)**.** As we have seen before,

$$M_{1,0}=M_{1,1}=\mathbb{A}^1 \quad (j\text{-line}).$$

Example 11.7 (Hyperelliptic curves, $\operatorname{char} k\neq 2$)**.** Recall that every hyperelliptic curve C of genus $g\geq 2$ admits a 2-to-1 map to $\mathbb{P}^1$, which is unique up to an automorphism of $\mathbb{P}^1$. In other words, C has a model

$$y^2=f(x), \qquad \deg f\in\{2g+1,2g+2\},\ \ f \text{ squarefree}.$$

The set of $2g+2$ roots of f (counting ∞ if $\deg f=2g+1$) is an element of $M^{\text{sym}}_{0,2g+2}$, so this is the space that classifies hyperelliptic curves of genus g up to isomorphism.

Exc 11.1. Prove that over an algebraically closed field, two elliptic curves are isomorphic if and only if they have the same j-invariant.

12. Representable functors

This is all well and good, but what does it really mean that X is a moduli space for a given classification problem? The bijection

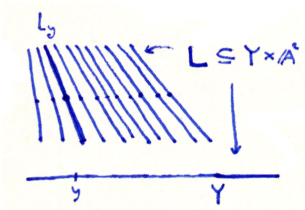
$$\{\text{our objects}/k\}/\cong \qquad \longleftrightarrow \qquad \text{set of points } X(k)$$

only specifies X as a set, and not as a variety. In the usual real or complex topology, we could appeal to continuity, and insist that 'close points' in the moduli space correspond to 'close objects'. In other words, if we have a continuous family of objects parametrised by some Y, then associating to every object the corresponding point of X gives a map $Y \to X$ that is continuous. This works perfectly well in the algebraic geometry setting, if we replace 'continuous map' by a 'morphism'.

Example 12.1. Recall that lines through the origin in $\mathbb{A}^2$ correspond to points of $\mathbb{P}^1$, via

$$ax + by = 0 \qquad \longleftrightarrow \qquad [a:b] \in \mathbb{P}^1_k.$$

Generally, a family of such lines over a variety Y corresponds to a unique morphism $Y \to \mathbb{P}^1$. Why is that? Well, for every point $y \in Y$ we have a line L_y that, together, form a closed subvariety L of $Y \times \mathbb{A}^2$:



Intersecting L with $Y \times \{(1,t)\}$, $Y \times \{(t,1)\}$ and projecting onto the second factors gives rational functions f and g, with $fg = 1$ and at least one of them regular at every point of Y. We get a morphism

$$Y \to \mathbb{P}^1, \qquad y \to [f(y):1] \quad (= [1:g(y)]).$$

And, conversely, it is easy to see that every morphism $Y \to \mathbb{P}^1$ comes from such a family. Moreover, the families over different varieties map to one another under morphisms: a morphism $f: X \to Y$ takes

$$\pi: L \to Y \qquad \longmapsto \qquad f^*\pi: L \times_Y X \to X,$$

where

$$L \times_Y X = \bigl\{(l,x) \in L \times X \bigm| \pi(l) = f(x)\bigr\} \qquad \text{(fibre product)}$$

is the *pullback* of the family L/Y under f.[35] Under the correspondence between families and maps to $\mathbb{P}^1$, this pullback simply corresponds to the composition with f,

$$f^*: \ \operatorname{Hom}(Y, \mathbb{P}^1) \qquad \longrightarrow \qquad \operatorname{Hom}(X, \mathbb{P}^1).$$

Lecture 7 The formal way of putting all this is that the two contravariant functors[36]

[35] This is a closed subset of $L \times X$, and so has a structure of an algebraic set.

$$\begin{array}{rccc} & \text{Varieties } /k & \longrightarrow & \text{Sets} \\ \mathcal{F}_1 : & Y & \longmapsto & \left\{ \begin{array}{c} \text{families of lines in } \mathbb{A}^2 \text{ through } 0 \\ \text{parametrised by } Y \end{array} \right\} / \cong \\ \mathcal{F}_2 : & Y & \longmapsto & \operatorname{Hom}(Y, \mathbb{P}^1) \end{array}$$

are isomorphic (called 'naturally equivalent').

Definition 12.2. A contravariant functor

$$\mathcal{F} : \text{Varieties } /k \quad \longrightarrow \quad \text{Sets}$$

is *representable*, or *representable by a variety* Y if $\mathcal{F} \cong \operatorname{Hom}(-, Y)$. The same definition applies to any category, and also for covariant functors, that are called representable if $\mathcal{F} \cong \operatorname{Hom}(Y, -)$.

Does this formalism really help? The short answer is 'YES'.

For example, take a family of lines in $\mathbb{A}^2$ through 0 parametrised by $C \setminus \{P\}$, where C is a curve and $P \in C$. Does it extend uniquely to a family over C? We showed that the functor 'families of lines through 0 in $\mathbb{A}^2$' is representable by $\mathbb{P}^1$, so this is equivalent to the question whether every morphism

$$C \setminus \{P\} \longrightarrow \mathbb{P}^1$$

extends to a unique morphism $C \to \mathbb{P}^1$. And we know the answer — since $\mathbb{P}^1$ is complete, it is yes if P is non-singular (and no in general). Basically, questions about families become questions about morphisms to a specific moduli space, and various properties of that moduli space, such as completeness, connectedness, dimension have a natural interpretation.

Here are a few other examples, all for the category of affine varieties $\mathbf{AVar}_k$. A contravariant functor $\mathbf{AVar}_k \to \mathbf{Sets}$ is the same as a covariant functor $\mathbf{Alg}_k \to \mathbf{Sets}$ on the category of finitely generated k-algebras with no nilpotents, so we construct these examples as functors of rings.

Example 12.3. Start with the 'forgetful' covariant functor $\mathbf{Alg}_k \to \mathbf{Sets}$ that takes a ring A to itself, considered as a set. For it to be representable means that there is some magic ring R with the property that

$$\operatorname{Hom}_{\mathbf{Alg}_k}(R, A) = A$$

as a set, for every k-algebra A. Such a ring exists, namely $R = k[x]$, because a homomorphism $k[x] \to A$ is uniquely determined by the image of x, which can be any element of A. Similarly

$$\begin{array}{lcll} \mathcal{F}(A) = \{\text{pairs of elements in } A\} & = & \operatorname{Hom}_{\mathbf{Alg}_k}(R, A), & R = k[x, y] \\ \mathcal{F}(A) = \{\text{4th roots of 1 in } A\} & = & \operatorname{Hom}_{\mathbf{Alg}_k}(R, A), & R = \frac{k[x]}{x^4 - 1} \\ \mathcal{F}(A) = \{\text{units in } A\} & = & \operatorname{Hom}_{\mathbf{Alg}_k}(R, A), & R = \frac{k[x,y]}{xy - 1}, \end{array}$$

[36] A *covariant* functor $\phi : \mathcal{C} \to \mathcal{C}'$ between two categories is a map on objects $\phi : \operatorname{Ob}(\mathcal{C}) \to \operatorname{Ob}(\mathcal{C}')$ and on morphisms $\operatorname{Hom}(A, B) \to \operatorname{Hom}(\phi(A), \phi(B))$ that preserves the category structure (identity morphisms and composition). A *contravariant* functor is the same except it reverses the arrows, taking $\operatorname{Hom}(A, B) \to \operatorname{Hom}(\phi(B), \phi(A))$.

so all the functors on the left[37] are representable. In other words, and this is just a tautology, a representable functor $\mathcal{F}$ in this setting is one for which $\mathcal{F}(A)$ can be given a structure of a set of solutions in A to a specific system of polynomial equations.

To give an example of a similar, but a non-representable functor, we can re-use the example of lines through the origin in $\mathbb{A}^2$, reformulated in terms of k-algebras (rather than affine varieties). Thus,

$$\mathcal{F}(A) = \bigl\{f, g \in A \bigm| fA + gA = A\bigr\}/A^\times.$$

It has two ‘subfunctors’,

$$\begin{array}{rcl} \mathcal{F}_1(A) &=& \bigl\{f, g \in A \bigm| fA + gA = A, f \text{ unit}\bigr\}/A^\times &=& \{g \in A\} \\ \mathcal{F}_2(A) &=& \bigl\{f, g \in A \bigm| fA + gA = A, g \text{ unit}\bigr\}/A^\times &=& \{f \in A\}, \end{array}$$

both represented by $k[t]$ (and their ‘intersection’ by $k[st]/(st-1)$). Passing from k-algebras to affine varieties, this just reflects the fact that $\mathbb{P}^1$ is not an affine variety, but it is covered with two $\mathbb{A}^1$s whose intersection is $\mathbb{A}^1 \setminus \{0\}$.

Going back to two examples

$$\begin{array}{lcll} \mathcal{F}_1(A) = \{\text{units in } A\} &=& \mathrm{Hom}_{\mathbf{Alg}_k}(R, A), & R = \frac{k[x,y]}{xy-1}, \\ \mathcal{F}_2(A) = \{\text{elements in } A\} &=& \mathrm{Hom}_{\mathbf{Alg}_k}(R, A), & R = k[x], \end{array}$$

there is, in this, case a ‘natural’ inclusion,

$$\mathcal{F}_1(A) = A^\times \hookrightarrow A = \mathcal{F}_2(A),$$

‘natural’ in the sense that it commutes with the maps $\mathcal{F}_i(A) \to \mathcal{F}_i(B)$ induces by homomorphisms $A \to B$. This inclusion corresponds to a map of representing rings

$$\begin{array}{ccc} k[x] & \longrightarrow & \frac{k[x,y]}{xy-1} \\ x & \longmapsto & x. \end{array}$$

(The map $x \mapsto y$ corresponds similarly to the inclusion $A^\times \hookrightarrow A, a \mapsto a^{-1}$.)

This is true in full generality, in any category. Maps between functors correspond exactly to morphisms between representing objects, by the following elementary result from category theory:

Theorem 12.4 (Yoneda’s lemma)**.** *For any category $\mathcal{C}$,*

$$A \longmapsto \mathrm{Hom}(A, -)$$

is a full embedding of $\mathcal{C}$ into the category of covariant functors $\mathcal{C} \to$ Sets.

Proof. Exc 12.1. □

‘Full embedding’ means precisely that every natural transformation of functors $\mathrm{Hom}(A, \cdot) \to \mathrm{Hom}(A', \cdot)$ is induced by a unique morphism $A' \to A$. In particular, if the two functors are isomorphic then $A \cong A'$, so the functor determines A. In particular, every moduli problem has at most a unique solution.

[37] made into covariant functors in the natural way

Note also that the definition of a representable functor does not rely in any way on k being algebraically closed, so we can talk about moduli problems over any base field K. For instance, the functor 'families of lines through 0 in $\mathbb{A}^2$' is representable on the category of algebraic sets over $\mathbb{Q}$, by $\mathbb{P}^1_{\mathbb{Q}}$. In particular, for any field $K \supset \mathbb{Q}$

$$\left\{ \begin{array}{c} \text{lines in } \mathbb{A}^2 \text{ through } (0,0) \\ \text{defined over } K \end{array} \right\} \quad \overset{1:1}{\longleftrightarrow} \quad \operatorname{Hom}(\operatorname{Spec} K, \mathbb{P}^1_{\mathbb{Q}}) = \mathbb{P}^1(K).$$

This suggests to define the set of *S-rational points* on any variety X for any algebraic set S,

$$X(S) = \operatorname{Hom}(S, X).$$

In this language, the $\operatorname{Hom}(-, X)$ functor that X represents is simply

$$S \ \longmapsto \ X(S) \qquad\qquad \text{(called 'functor of points')}.$$

Yoneda's lemma says that X is uniquely determined by its functor of points, and moduli problems become questions whether a given functor is a functor of points on some variety. If $S = \operatorname{Spec} A$ is affine, we write $X(A) = X(S)$, and for fields this defines K-rational points as we had before.

Example 12.5 (Product of varieties)**.** Naively, the product $V \times V'$ of two varieties is a variety whose points are pairs of points (v, v'). This only describes it as a set, and there are two psychologically different ways to think of its structure as a variety and to deduce its properties (the existence of natural projections to V and to V', associativity $(V \times V') \times V'' = V \times (V' \times V'')$, etc.)

The 'constructive' approach is what we followed before: pass to $\bar{k}$, and suppose first $V \subset \mathbb{A}^n$ and $V' \subset \mathbb{A}^{n'}$ are affine. Then $V \times V' \subset \mathbb{A}^{n+n'}$ is clearly an algebraic set. It happens to be irreducible, so $V \times V'$ becomes an affine variety; for general V, V', we glue the pairwise products of affine charts, and prove that this works and is independent of any choices. The properties such as associativity are then deduced from this (somewhat cumbersome) construction.

The 'functorial' approach is simply to demand the naive 'pairs of points' description, but for *all* varieties S; thus, $V \times V'$ is defined as a variety that represents the product functor[38]

$$S \longmapsto V(S) \times V'(S).$$

If such a variety $V \times V'$ actually exists, its properties are deduced from Yoneda's lemma; e.g. $(V \times V') \times V''$ and $V \times (V' \times V'')$ have the same functor of points, so there is a canonical isomorphism between them; the first projection map

$$V(A) \times V'(A) \to V(A)$$

is a natural transformation from the functor of points of $V \times V'$ to that of V, so by Yoneda's lemma it comes from a unique variety map $V \times V' \to V$; etc.

[38] and this is how products can be defined in any category, not just for varieties

Example 12.6 (Algebraic groups)**.** In any category $\mathcal{C}$, we can define a 'group object' as one for which the functor

$$\mathrm{Hom}(-,X):\ \mathcal{C}\longrightarrow \textbf{Sets}$$

factors through the category of groups. In other words $X(S)$ is a group for every object $S\in\mathcal{C}$, and all $X(S)\to X(T)$ are group homomorphisms. Using Yoneda's lemma, it is not hard to check that in the category of varieties this defines (connected) algebraic groups, as we defined them.

It is an important unsolved question in algebraic geometry how to characterise representable functors in some sort of intrinsic way. There are categories where there are such necessary and sufficient criteria for functors to be representable, but for varieties (or schemes) this seems to be very hard.

Exc 12.1. Prove Yoneda's lemma.

13. Hilbert scheme and standard moduli spaces

We started with several examples — families of lines and conics in the plane, and the corresponding functors turn out to be representable. They are special cases of the fundamental construction, the *Hilbert scheme*, that classifies closed subsets of $\mathbb{P}^n$ (or of any projective variety) with given discrete invariants specified by the *Hilbert polynomial*:

A closed subset $Z\subset\mathbb{P}^n$ is a zero set of a homogeneous ideal $I\subset k[x_0,...,x_n]$, and its homogenous coordinate ring splits into degree d graded pieces,

$$S=k[x_0,...,x_n]/I=\bigoplus_{d\geq 0}S_d.$$

Consider the dimension counting function (the *Hilbert function*)

$$d\quad\longmapsto\quad \dim_k S_d.$$

Example 13.1 (Point)**.** If $Z=\{[1:0:\ldots:0]\}\subset\mathbb{P}^n$ is a point, then

$$I=(x_1,...,x_d),\ \ S=k[x_0],\qquad \dim_k S_d=(1,1,1,1,\ldots)$$

Example 13.2 (Linear subspaces)**.** If $Z=\mathbb{P}^m\subset\mathbb{P}^n$, then $S=k[x_0,...,x_m]$,

$$\dim_k S_d=\tbinom{d+m}{m}=\frac{1}{m!}\,d(d-1)\ldots(d-m+1).$$

Example 13.3 (3 points in $\mathbb{P}^2$)**.** A bit more interesting example is subsets

$$\{P_1,P_2,P_3\}\subset\mathbb{P}^2$$

of three distinct points. The coordinate ring $S=k[x,y,z]/I$ depends on whether the points are collinear or not. Fixing a choice of coordinates for the P_i, it is clear that

$$k[x,y,z]_1\longrightarrow k^3,\qquad f\mapsto(f(P_1),f(P_2),f(P_3))$$

is onto if the P_i are not collinear, and has 2-dimensional image otherwise. So $\dim I_1 = 0, \dim S_1 = 3$ in the former case, and $\dim I_1 = 1, \dim S_1 = 2$ in the latter. And for every $d \geq 2$ it is easy to check that

$$k[x,y,z]_d \longrightarrow k^3, \qquad f \mapsto (f(P_1), f(P_2), f(P_3))$$

is always onto, and $\dim S_d = 3$. In other words, there always exist degree d homogeneous polynomials f_1, f_2, f_3 such that $f_i(P_j) = \delta_{ij}$, whatever the three points are. So

$$\begin{array}{ll} \dim_k S_d = (2,3,3,3,\dots) & \text{if the } P_i \text{ are collinear,} \\ \dim_k S_d = (3,3,3,3,\dots) & \text{if the } P_i \text{ are not collinear.} \end{array}$$

The Hilbert-Serre theorem asserts that for every algebraic set $Z \subset \mathbb{P}^n$, if we write I for the ideal of functions vanishing on Z and $S = k[x_0,...,x_n]/I$ for its homogeneous coordinate ring, the sequence $\dim S_d$ always stabilises for large enough d to coincide with values of a unique polynomial $H_Z(d)$, whose degree is the dimension of Z.

Definition 13.4. $H_Z(d)$ is the *Hilbert polynomial* of Z, and its leading coefficient times $(\dim Z)!$ is the *degree* of Z in $\mathbb{P}^n$.

Example 13.5.

$$\begin{array}{llll} Z = \{\text{pt}\} & \Rightarrow & H_Z(d) = 1 & (\deg Z = 1) \\ Z = \mathbb{P}^m & \Rightarrow & H_Z(d) = \frac{1}{m!}\, d(d-1)\dots(d-m+1) & (\deg Z = 1) \\ Z = \{P_1, P_2, P_3\} & \Rightarrow & H_Z(d) = 3 & (\deg Z = 3). \end{array}$$

For a hypersurface $H = 0$ in $\mathbb{P}^n$ the degree is $\deg H$, as we had before.

Theorem 13.6. *For every polynomial $H(d)$, the functor*

$$\underline{\text{Hilb}}_{\mathbb{P}^n,H} : \ S \ \longmapsto \ \begin{array}{c} \textit{families } Y \subset S \times \mathbb{P}^n \textit{ of closed subsets of } \mathbb{P}^n \\ \textit{with Hilbert polynomial } H(d) \textit{ over } S \end{array}$$

is representable by a projective scheme[39] $\text{Hilb}_{\mathbb{P}^n,H}$.

Other closely related functors are:

- $\underline{\text{Hilb}}_{\mathbb{P}^n} = \coprod_H \underline{\text{Hilb}}_{\mathbb{P}^n,H}$,

the functor that classifies all closed subsets of $\mathbb{P}^n$ (or, rather, flat families of them as we will define shortly). It can be extended from $\mathbb{P}^n$ to any projective variety X as well,

- $\underline{\text{Hilb}}_X$ = functor of (flat) families of closed subvarieties of X

Next, since we can view a morphism from X to Y, as a closed subvariety of $X \times Y$, via its graph, for projective varieties X and Y we can consider

- $\underline{\text{Hom}} : T \mapsto \text{Hom}_T(X \times T, Y \times T)$ (open $\subset \text{Hilb}_{X \times Y}$)
- $\underline{\text{Isom}} : T \mapsto \text{Isom}_T(X \times T, Y \times T)$ (open $\subset$ Hom)
- $\underline{\text{Aut}} : T \mapsto \text{Aut}_T(X \times T)$ (take $X = Y$)

All these functors are always representable (by a scheme). The proof of representability is not overly hard. Like for NP-completeness, when you do the hard work once for one problem and then reduce all the others to it.

[39] It is not always a variety, and can be highly singular

First, one proves representability for a slight extension of the Hilbert scheme functor, called $\mathrm{Quot}_{X,\mathcal{M}}$, that parametrises quotients of a coherent sheaf on X. (Subvariety of a projective space is given by a homogeneous inside its coordinate ring, and an arbitrary coherent sheaf is a generalisation of this.) Grothendieck proved that it is representable by reducing it to the classical Grassmanian, by using embeddings into large projective spaces to reduce the question to that for linear subspaces. Then representability of all the other functors is a consequence of that one.

Finally, another important one is the Picard functor, that parametrises families of divisors on a variety:

- $\underline{\mathrm{Pic}} : T \mapsto \mathrm{Pic}_T(X \times T)/\operatorname{Pic} T$.

In favourable situations, it is representable as well, e.g. for complete varieties (over any field K) that have a K-rational point.

Example 13.7. If C/K is a complete non-singular curve, with $C(K) \neq \emptyset$, then $\mathrm{Pic}(C)$ is representable by a scheme, which is naturally a group. Its connected component $\mathrm{Pic}^0(C)$ is represented by a projective commutative algebraic group, in other words an abelian variety. It has dimension equal to the genus of C, and is called the *Jacobian variety* of C, ofted denoted $\mathrm{Jac}(C)$ as well.

Example 13.8 (Albanese)**.** Another type of functors attempts to find a canonical 'closest' object to a given one in a different category. One classical example (another, much simpler one, is Exc 13.1) is the *Albanese* functor that finds an abelian variety closest to a given variety, in the following sense. Let V/K be a non-singular projective variety with a base point $P_0 \in V(K)$, and consider the functor

$$\begin{array}{rccc} \mathcal{F}: & \mathbf{AbVar}_K & \longrightarrow & \mathbf{Sets} \\ & A & \longmapsto & \mathrm{Hom}_0(V, A), \end{array}$$

from abelian varieties over K to sets, where where Hom_0 stands for morphisms of varieties that map P_0 to 0. It turns out that it is representable, and the representing variety is called the *Albanese variety* $\mathrm{Alb}(V)$ *of* V. In other words, it is an abelian variety with a morphism (taking P_0 to 0)

$$f : V \to \mathrm{Alb}(V),$$

which is universal, in the sense that any other such morphism from V to any abelian variety over K factors uniquely through f.

For non-singular projective curves Albanese coincides with the Jacobian (i.e. Pic^0), and the unversal map

$$f : C \to \operatorname{Pic}^0 C$$

takes P to the divisor $(P) - (P_0)$.

Exc 13.1. Suppose G is any finite group, and consider the following functor from the category of finite *abelian* groups to sets,

$$\begin{array}{rccc} \mathcal{F}: & \mathbf{Ab} & \longrightarrow & \mathbf{Sets} \\ & A & \longmapsto & \mathrm{Hom}(G, A). \end{array}$$

Prove that $\mathcal{F}$ is representable, and describe the representing object.

14. Flat families

Grothendieck's advice is to always work in the relative setting. A variety is really a morphism $V \to \{\mathrm{pt}\}$, a special case of a family $\mathcal{V}$ over an arbitrary base S. In particular, the most important properties for algebraic set over a field have relative analogues: a non-singular V/k generalises to a *smooth morphism* $\mathcal{V} \to S$, complete V/k to a *proper morphism*, and finite V to a *finite morphism.*

Definition 14.1. A morphism $f : X \to Y$ is

- *smooth* (of relative dimension d) if $\hat{O}_{X,x} \cong \hat{O}_{Y,y}[[t_1, ..., t_d]]$ for every pair of points $f(x) = y$. Equivalently, f is flat with regular fibres[40].
- *proper* if f is universally closed, that is $f_Z : X \times Z \to Y \times Z$ is closed for every variety Z.
- *finite* if Y has an affine cover

  $$Y = \bigcup \operatorname{Spec} B_i, \qquad f^{-1}(\operatorname{Spec} B_i) = \operatorname{Spec} A_i \text{ affine},$$

  with A_i finitely generated B_i-modules; equivalently, f is proper with finite fibres.

The correct (for somewhat mysterious reasons) notion of a nice general family of varieties turns out to be *flatness*[41].

Definition 14.2. For a ring A, an A-module M is *flat* if $I \otimes_A M \to IM$ is an isomorphism for every ideal $I \subset A$.

Definition 14.3. A morphism $f : X \to Y$ is *flat* [of relative dimension d] if Y has an affine cover

$$Y = \bigcup \operatorname{Spec} B_i, \qquad f^{-1}(\operatorname{Spec} B_i) = \operatorname{Spec} A_i \text{ affine},$$

with A_i *flat* B_i-modules. (Flatness implies that all non-empty fibers have the same dimension $d = \dim X - \dim Y$.)

All four notions enjoy a host of good properties, such as being preserved under composition and base change.

Example 14.4. The projections $X \to \{\mathrm{pt}\}$ and $X \times Y \to Y$ are flat; they are proper $\Leftrightarrow$ X is complete, and smooth $\Leftrightarrow$ X is non-singular.

Example 14.5.

- Closed immersions $Z \hookrightarrow Y$ are finite ($\Rightarrow$proper).
- Open immersions $U \hookrightarrow Y$ are smooth ($\Rightarrow$flat).

[40] regular scheme-theoretic fibres, to be precise

[41] Introduced by Serre but made into a cornerstone of families by Grothendieck

Theorem 14.6 (Flatness criteria)**.**

(1) If $X \subset Y \times \mathbb{P}^n$ is closed, then the projection $X \to Y$ is closed if and only all fibers $X_y \subset \mathbb{P}^n$ have the same Hilbert polynomial.

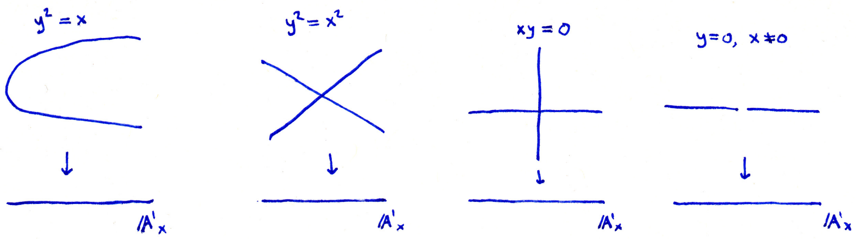
(2) A finite *morphism $f : X \to Y$ is flat if and only if it is locally free of finite rank, in other words the rings A_i, B_i in the definition of finiteness can be chosen with A_i finitely generated and* free *over B_i.*

(3) A morphism $f : X \to Y$ between regular *varieties is flat iff*

$$\dim X = \dim Y + \dim O_x/m_y O_x$$

for all points $f(x) = y$ (with local rings O_x, O_y and maximal ideals m_x, m_y).

Example 14.7. Of the following four varieties, the first two are finite and flat over $\mathbb{A}^1_x$, the third one is neither, and the last one is flat but not finite.



For the first two, their coordinate rings are $k[x] \oplus k[x]y$ as $k[x]$-modules, that is free finitely generated of rank 2. The fourth one is an open immersion, while the third one has fibers of varying dimension.

Example 14.8. Of the two surfaces

$$S_1 : y^2 = x^3 - t, \qquad\qquad S_2 : ty^2 = tx^3 - t,$$

the first one is flat over the t-line $\mathbb{A}^1_t$, and the second one is not. For the first one, the morphism factors $S_1 \longrightarrow \mathbb{A}^2_{t,x} \longrightarrow \mathbb{A}^1_t$, with the first map finite flat by 14.6(2) and the second one flat by 14.4. It is not proper (non-complete fibres) and not smooth (singular fibre at $t = 0$). As for S_2, the $t = 0$ fibre is $\mathbb{A}^2$, while all the others have dimension 1.

Example 14.9.

- If A is a field, every A-module is flat.
- An A-module M is flat iff the localisation M_P is A_P-flat for every prime (equivalently maximal) ideal $P \subset A$.
- Suppose $A \to B$ is a flat local homomorphism of Noetherian local rings, and $b \in B$. Then $A \to B/(b)$ is flat if and only if the image of b in $B/m_A B$ is a non-zero divisor.
- If A is a PID, flat is equivalent to torsion-free.

Example 14.10. $B = k[x,y]/xy$ as a $k[x]$-module. Use maximal ideal criterion: for every maximal $m = (x - a) \subset k[x]$ with $a \neq 0$, the localization B_m is free of rank 1 over A_m (and is therefore flat), but for $a = 0$ the localization B_m is $k[x]_m[y]/xy$ which is not flat, as y is x-torsion.

Exc 14.1. (projective) version of Example 14.8. And smooth as well.

15. Moduli space of curves

Now that we have a good notion of a family, we can define the moduli space of curves:

Definition 15.1. Let K be a field, and S an algebraic set over K. A *curve $\mathcal{C}/S$ of genus g* is a flat morphism $\pi : \mathcal{C} \to S$ whose geometric[42] fibers are (non-singular projective) curves of genus g.

An *n-pointed curve* is $(\mathcal{C};\, \mathcal{P}_1, \ldots, \mathcal{P}_n)$ where $\mathcal{P}_i$ are sections $S \to \mathcal{C}$ of π, disjoint over every point of $S/\bar{K}$.

Definition 15.2. For $g, n \geq 0$ define the functors $\mathbf{AlgSets}_K \to \mathbf{Sets}$,

$$\begin{array}{lrcl} \mathcal{M}_g : & S & \longmapsto & \{\text{curves of genus } g \text{ over } S\}/\cong . \\ \mathcal{M}_{g,n} : & S & \longmapsto & \{n\text{-pointed curves of genus } g \text{ over } S\}/\cong . \end{array}$$

These are very important functors, and the only trouble with them is that they are, unfortunately, *not* representable in general. Here are two examples:

Example 15.3 ($g = 0, n = 2$, lines through 0)**.** Every genus 0 curve with two marked points $(C; P_1, P_2)$ over any field K is isomorphic to $(\mathbb{P}^1; 0, \infty)$, though not uniquely. There is a group of non-trivial automorphisms $\mathbb{G}_m$ ($x \mapsto tx$) acting on $(\mathbb{P}^1; 0, \infty)$, and it turns out that these automorphisms cause problems for representability.

If the functor $\mathcal{M}_{0,2}$ is representable by some variety $M_{0,2}$, then

$$M_{0,2}(K) = \mathcal{M}_{0,2}(\operatorname{Spec} K) = \{\text{one point}\}$$

for any field K, so $M_{0,2} = \{\text{pt}\}$. However, this would imply that $\mathcal{M}_{0,2}(S) = \{\text{one point}\}$ for any base S, in other words every *family* $\mathcal{C}$ of curves with 2 marked points over any base S must be trivial,

$$\mathcal{C} \;\cong\; S \;\times\; \mathbb{P}^1 \backslash \{0, \infty\}.$$

But this is not true — look at the tautological family of lines over $\mathbb{P}^1_{\mathbb{R}}$ which is the Möbius band. (Topologically not orientable.)

The problem is clearly glueing via an automorphism $x \mapsto -x$. Generally in the topological setting have trivial families over disks, but $H^1(\pi_1(S), \mathrm{Aut})$ measures the obstruction, and is $H^1(\mathrm{Gal}, \mathrm{Aut})$ that we have seen before. [This is referred to as *monodromy*.]

Example 15.4 ($g = n = 1$, elliptic curves)**.** Let $g = n = 1$, say $\operatorname{char} K \neq 2$, and suppose that $\mathcal{M}_{g,n} \cong \mathrm{Hom}(-, M)$ for some moduli space M, e.g. the j-line. Take any elliptic curve

$$E/K : y^2 = f(x)$$

[42] that is fibers over the points of $S/\bar{K}$

and all of its quadratic twists

$$E_d/K : dy^2 = f(x), \qquad d \in K^\times/K^{\times 2}.$$

They are all pairwise non-isomorphic over K, so each would give a different point in $M(K)$. But they are all isomorphic over $\bar{K}$, so these points should become the same in $M(\bar{K})$! This is impossible. And this is not just a problem with non-algebraically closed fields — such an example over a function field breaks always representability. So, even if $k = \bar{k}$, the two families

$$E_1/\mathbb{A}^1_t : y^2 = f(x) \qquad \text{and} \qquad E_t/\mathbb{A}^1_t : ty^2 = f(x)$$

are non-isomorphic over $k[t]$ but are isomorphic over $k[\sqrt{t}]$ (i.e. become isomorphic under the pullback $k[t] \to k[t]$, $t \mapsto t^2$), and this is again impossible, because two morphisms

$$\mathbb{A}^1 \longrightarrow M$$

cannot become the same after the composition with $\mathbb{A}^1 \to \mathbb{A}^1$, $t \mapsto t^2$. So the j-invariant is a good invariant over algebraically closed fields, but it does not work to classify families.

Grothendieck observed (in a 1959 letter to Serre) that, at least morally, this problem would always occur if we attempt to classify objects that have non-trivial automorphisms. Topologically, it is easy to see why it happens by looking at families (of anything, really) over a unit circle S^1.

The classical example is a Möbius band: it is a family of 1-dimensional $\mathbb{R}$-vector spaces (lines) parametrised by S^1. Every such family over $U = S^1 \setminus \{\text{pt}\}$ is trivial, i.e. isomorphic to $U \times \mathbb{R}^1$. However, there are different ways to glue the ends and extend such a trivial family to a family over S^1 — 'straight' or 'upside down'. In other words, going around in a loop over S^1 is an automorphism of a fibre, and if this automorphism is non-trivial, the family is not trivial either. If all the fibres are the same, such families preclude the existence of a moduli space. In fact, we have already seen that twists of varieties or algebraic groups are classified by $\text{Gal}(\bar{K}/K, \text{Aut}_{\bar{K}} V)$, with $\text{Gal}(\bar{K}/K)$ playing the role of the fundamental group of the unit circle in our setting.

This means that interesting spaces very often do not exist, as the corresponding functors are not representable.

Solution 1 is to weaken the definition of a moduli space. We say that a variety M/K is a *coarse moduli space* for a functor

$$\mathcal{M} : \mathbf{AlgSets}_K \to \mathbf{Sets}$$

if there is a natural transformation of functors $\phi : \mathcal{M} \to \text{Hom}(-, M)$ so that

1. $\mathcal{M}(\bar{K}) \to M(\bar{K})$ is a bijection, and
2. For any V/K, every natural transformation $\psi : \mathcal{M} \to \text{Hom}(-, V)$ factors uniquely through ϕ.

The first property says that at least over $\bar{K}$ the moduli space classifies what it is supposed to classify, and the second guarantees its uniqueness (if it exists). Of course, if $\mathcal{M}$ is representable, then the representing algebraic set V (also called a *fine moduli space*) is also a coarse moduli space.

In the case of $\mathcal{M}_{g,n}$ this works well, and the coarse moduli space $M_{g,n}$ exists for all g and n. In particular, $M_{1,0} = M_{1,1}$ is the j-line $\mathbb{A}^1/K$. In this case, the natural transformation $\mathcal{M}_{1,1} \to \mathrm{Hom}(-, \mathbb{A}^1)$ takes a family $\mathcal{E}/S$ and associates to the j-invariant map on fibers $j(\mathcal{E}) : S \to \mathbb{A}^1$.

The disadvantage of this approach is that coarse moduli space is simply not good enough to understand families of curves properly. For example, we constructed a family of curves

$$E_j : y^2 + xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728} \quad \text{over} \quad \mathbb{A}^1_j \setminus \{0, 1728\}.$$

Does it extend to a family over the whole j-line? By definition of the coarse moduli space, we have a morphism

$$\mathbb{A}^1_j \setminus \{0, 1728\} \quad \longrightarrow \quad \mathbb{A}^1_j,$$

the natural inclusion. It extends to the identity map $\mathbb{A}^1_j \to \mathbb{A}^1_j$, but this does not imply existence (or uniqueness) of a family over $\mathbb{A}^1$, as

$$\mathcal{M}_{1,1}(\mathbb{A}^1) \longrightarrow \mathrm{Hom}(\mathbb{A}^1, \mathbb{A}^1)$$

may neither be injective nor surjective. (In fact, it turns out that such an extension does not exist in this case.)

Solution 2 is to *rigidify* the problem to get rid of automorphisms. For instance, a curve C/k of genus 0 has a large automorphism group (the Möbius group $\mathrm{PGL}_2(k)$), but a curve with a marked point (C, P_1) has less ($\cong k \rtimes k^\times$), with two marked points less still ($\cong k^\times$), and with three or more marked points no non-trivial automorphisms. And, indeed, it turns out that $\mathcal{M}_{0,n}$ is representable for $n \geq 3$, by the varieties that we have seen before,

$$M_{0,3} = \{\mathrm{pt}\}, \qquad M_{0,4} = \mathbb{P}^1 \setminus \{0, 1, \infty\}, \qquad \text{etc.}$$

The same works for any genus g, and large enough n depending on g. The functors $\mathcal{M}_{g,n} \to \mathcal{M}_g$ ('drop the points') give maps of varieties $M_{g,n} \to M_g$. This in principle allows us to study families of curves by going back and forth between the variety M_g that we want and $M_{g,n}$ that has better functorial properties.

Adding points is not the only, and possibly not the best solution, as it increases the dimension of moduli spaces. For example, $\dim M_{1,n} = n$, and it is a fine moduli space for $n \geq 5$, by which time the geometry of it becomes quite unmanageable, especially if compared to the j-line $\mathbb{A}^1$. One standard way that works very well for elliptic curves (and abelian varieties) and is to add a *level structure*. The subgroup $E[n]$ of n-torsion points on an elliptic curve E/k is

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 \qquad (\mathrm{char}\, k \nmid n),$$

and choosing an isomorphism with a fixed copy of $(\mathbb{Z}/n\mathbb{Z})^2$ provides enough 'rigidity' to get rid of all automorphisms. Even fixing one n-torsion point is enough, for $n \geq 3$, and the corresponding (fine) moduli spaces are called modular curves $X_1(n)$ (fix one n-torsion point) and $X(n)$ (fix the whole of $E[n]$).

Solution 3, perhaps the most natural one, is to extend the category of varieties (or schemes) to a larger one where the functor does become representable, but still geometrically manageable[43]. Such extensions exist — this is the theory of algebraic spaces and stacks. They did prove to be useful, although the theory is highly technical, the are many different incarnations of stacks, and the subject seems to be hard to get into.

References

[Bak] H. F. Baker, Examples of applications of Newtons polygon to the theory of singular points of algebraic functions, Trans. Cambridge Phil. Soc. 15 (1893), 403–450.

[BP] P. Beelen, R. Pelikaan, The Newton polygon of plane curves with many rational points, Designs, Codes and Cryptography 21 (2000), 41–67.

[Can] D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve, Math. Comp. 48 (1987), 95–101.

[H] R. Hartshorne, Algebraic Geometry, GTM 52, Springer 1977.

[KWZ] A. Kresch, J. L. Wetherell, M. E. Zieve, Curves of every genus with many points, I: abelian and toric families, J. Algebra 250 (2002), 353–370.

[Sil1] J. H. Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag 1986.

[Wat] W. Waterhouse, Introduction to affine group schemes, GTM 66, Springer 1979.

[43] We could embed $\mathbf{Var}_k$ into the category of functors $\mathbf{Var}_k \to \mathbf{Sets}$ and that would make every functor on $\mathbf{Var}_k$ representable, by definition. But proving anything useful in this larger category seems to be hopeless.

Assignments.

Problem 1. Take the following curves in $\mathbb{A}^2_{x,y}$

$$C : y^2 = x^3, \qquad D : y^2 = x^3 + x^2, \qquad E : y^2 = x^3 + x,$$

Prove that the completed local rings at $p = (0, 0)$ are

$$\hat{\mathcal{O}}_{C,p} \cong k[[t^2, t^3]], \qquad \hat{\mathcal{O}}_{D,p} \cong k[[s, t]]/st, \qquad \hat{\mathcal{O}}_{E,p} \cong k[[t]],$$

and that they are pairwise non-isomorphic when $\operatorname{char} k \neq 2$.

Problem 2.

(1) Show that $\mathbb{P}^1 \times \mathbb{P}^1 \ncong \mathbb{P}^2$. (You may want to use 'weak Bezout'.)

(2) If V is any variety, a rational map $f : V \rightsquigarrow \mathbb{P}^n$ is given by $n + 1$ rational functions $f_0, ..., f_n \in k(V)$ (not all identically zero on V),

$$V \ni P \quad \longmapsto \quad [f_0(P) : ... : f_n(P)] \in \mathbb{P}^n,$$

and $gf_0, ..., gf_n$ give the same map, for $g \in k(V)^\times$. If, for a point $P \in V$, there is such a g that the gf_i are all defined and not all zero at P, we say that f is regular (or defined) at P, and $f(P)$ is the corresponding value. Use this to show that $\mathbb{P}^n$ is complete, by verifying the valuative criterion.

Problem 3. Suppose C/k is a complete non-singular curve that admits a map $x : C \to \mathbb{P}^1$ of degree 2, in other words C is hyperelliptic. For simplicity, assume $\operatorname{char} k = 0$.

(1) Show that C is birational to a curve $y^2 = f(x) \subset \mathbb{A}^2$, with $f \in k[x]$ square-free. (Hint: Describe $k(C)$.)

(2) Conversely, if $f(x) \in k[x]$ is squarefree, of degree $2g + 1$ or $2g + 2$, for some $g > 0$, the two affine charts

$$y^2 = f(x) \qquad \text{and} \qquad Y^2 = X^{2g+2} f(\tfrac{1}{X})$$

glue via $Y = \frac{y}{x^{g+1}}$, $X = \frac{1}{x}$ to a complete, non-singular curve C. (You may use this.) Show that C has genus g, with regular differentials

$$\Omega_C = \Big\langle \frac{dx}{y}, \frac{xdx}{y}, \ldots, \frac{x^{g-1}dx}{y} \Big\rangle.$$

Now let C be *any* complete non-singular curve of genus 2. Use $\deg K_C = 2$ and $\dim \mathcal{L}(K_C) = 2$ to prove that C is hyperelliptic.

Problem 4. Suppose C/k ($\operatorname{char} k \neq 2$) is a hyperelliptic curve of genus $g \geq 1$, given by an equation

$$y^2 = x^{2g+1} + a_{2g}x^{2g} + \ldots + a_0.$$

Write ∞ for the unique point at infinity of C.

(1) Use Cantor's description of divisors to describe the 2-torsion elements (elements of order 2) in $\operatorname{Pic}^0(C)$. Show that they form a group $\cong \mathbb{F}_2^{2g}$, and describe how to add them explicitly.

(2) Suppose $P \in C \cap \mathbb{A}^2$ is a 'torsion point of order $2g+1$', in the sense that the divisor $D = (P) - (\infty)$ is $(2g+1)$-torsion,

$$(2g+1)D \sim 0.$$

E.g. by considering the function $f \in \mathcal{L}((2g+1)(\infty))$, that defines the latter equivalence, its image under the hyperelliptic involution, and the natural basis of $\mathcal{L}((2g+1)(\infty))$, show that C has an equation of the form

$$y^2 = x^{2g+1} + (b_g x^g + \ldots + b_1 x + b_0)^2.$$

(This illustrates the fact that high-order torsion points on curves are rare.)

Problem 5.

1. Prove that $\operatorname{Aut}\mathbb{P}^1 \cong \mathrm{PGL}_2(k)$.
2. Find $\operatorname{Aut}\mathbb{A}^1$ and $\operatorname{Aut}(\mathbb{A}^1 \setminus \{0\})$.
3. Find $\operatorname{Aut}\mathbb{G}_m$ (isomorphisms $\mathbb{G}_m \to \mathbb{G}_m$ as an algebraic group).

Problem 6.

1. Prove that over $K = \mathbb{R}$, the unit circle group $S^1 : x^2 + y^2 = 1$ is the only non-trivial form of $\mathbb{G}_m$ up to isomorphism (as algebraic groups).
2. Similarly, over $K = \mathbb{F}_p$, prove that $\mathbb{G}_m$ has a unique non-trivial form. Write it down an an algebraic group (equations + structure morphisms), and determine its number of points over K.

Problem 7. In any category $\mathcal{C}$, we can define a 'group object' as one for which the functor

$$\operatorname{Hom}(-, X) : \ \mathcal{C} \longrightarrow \textbf{Sets}$$

factors through the category of groups. Prove that group objects in the category of varieties are (connected) algebraic groups, as we defined them.